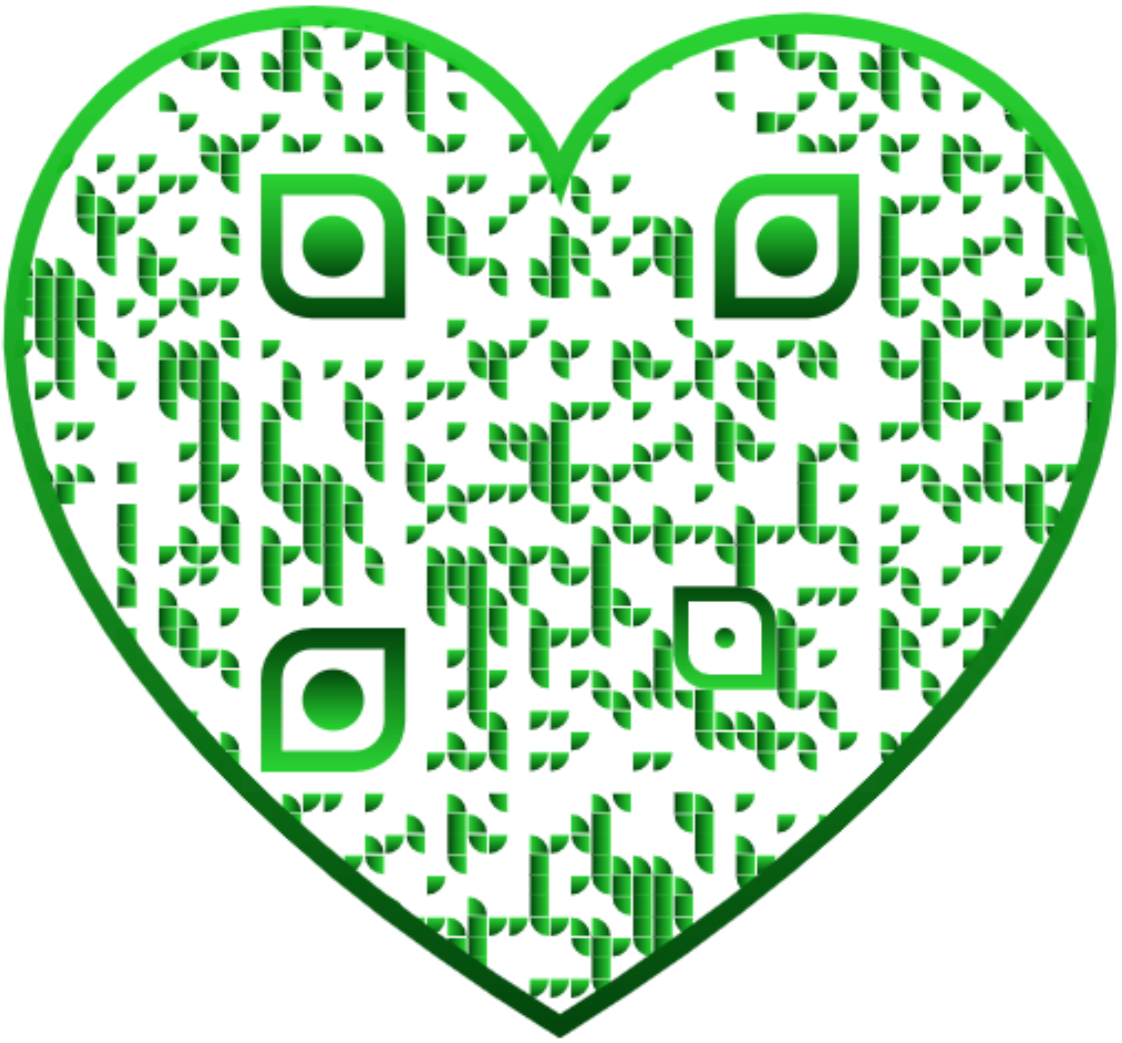
Stéphane Loignon

BIG BANG BLOCKCHAIN

LA SECONDE RÉVOLUTION D'INTERNET

Tallandier



Stéphane Loignon

BIG BANG BLOCKCHAIN

La seconde révolution d'Internet

TALLANDIER

© Éditions Tallandier, 2017
2, rue Rotrou – 75006 Paris

www.tallandier.com

EAN : 979-10-210-2270-6

Ce document numérique a été réalisé par Nord Compo.

À Sophie, l'amour de ma vie.

Sommaire

Titre

Copyright

Dédicace

Préface

Prologue - Retour vers le futur post-blockchain

Introduction - La seconde révolution d’Internet

Préambule - Une brève histoire de la blockchain

Première partie - COMMENT FONCTIONNE UNE BLOCKCHAIN ?
- Chapitre premier - Qu’est-ce qu’une blockchain ?
- Chapitre 2 - Les mécanismes du consensus
- Chapitre 3 - Caractéristiques des blockchains

Deuxième partie - QUELLES FUTURES APPLICATIONS ?
- Chapitre 4 - Une révolution financière
- Chapitre 5 - Une vraie économie du partage
  - Objectif : bousculer les géants du Web
  - Musique, culture et médias : rendre le pouvoir à ceux qui créent
  - Jouer, parier et deviner l’avenir
- Chapitre 6 - Un tremplin vers un monde automatisé
- Chapitre 7 - Un pilier pour la démocratie et l’administration de demain
  - Réinventer la démocratie

Repenser les services de l’État

Un cyberoffice notarial

Troisième partie - LES DÉFIS DE LA BLOCKCHAIN

Chapitre 8 - Développer des systèmes moins énergivores

Chapitre 9 - Rapidité, confidentialité, sécurité : trois défis techniques

Chapitre 10 - Marketing : trouver des modèles économiques viables sans se renier

Chapitre 11 - Transformer l’emploi sans le détruire

Chapitre 12 - Réglementer sans freiner l’innovation

Chapitre 13 - Une question de souveraineté pour la France et l’Europe

Conclusion

Notes

Remerciements

Du même auteur

Préface

La technologie « blockchain » aura sans conteste été la révélation de l'année 2016 pour le grand public. La multiplication d'articles publiés et d'événements organisés sur ce sujet est à la mesure de la révolution culturelle, sociétale et même politique que cette innovation pourrait préfigurer.

Via l'automatisation et une décentralisation radicale des mécanismes de contrôle et de sécurité des échanges, les chaînes de bloc pourraient, demain, affecter en profondeur les conditions de production et d'échange d'énergie, de flux financiers ou de biens dans notre économie. Cette technologie pourrait remettre en cause tout le modèle de société dans lequel nous vivons. Banques, assurances, places financières et de marchés, États et administrations publiques : la légitimité de la superstructure, cet ensemble de systèmes centralisés dont parlait Karl Marx, pourrait s'effacer au profit d'une économie radicalement décentralisée et collaborative. Dans le domaine de l'énergie, le jour, imaginé par Jeremy Rifkin, où producteurs et consommateurs ne feront plus qu'un au sein de communautés locales de production d'énergie fédérées dans des réseaux intelligents, ou *smart grids*, vendant ou achetant de l'électricité ou des énergies renouvelables en fonction de leurs besoins, ne paraît plus si éloigné…

Derrière ces horizons de long terme qui peuvent séduire et inquiéter, se profilent des choix politiques majeurs que nous devons d'ores et déjà anticiper… sans pour autant négliger les applications concrètes et utiles qui se développent actuellement. D'une manière générale, tous les secteurs où la fiabilité des données, la preuve de l'identité, la propriété et la normalisation sont des objectifs clés peuvent bénéficier de la blockchain. Dans le secteur bancaire, son utilisation est synonyme de baisse des coûts et d'accélération des transactions, ou encore d'amélioration de la lutte contre la fraude. Son potentiel pourrait s'étendre demain à la santé publique et permettre une amélioration considérable de la traçabilité des médicaments. Enfin, à l'heure du développement du vote électronique, notamment au profit de nos compatriotes établis à l'étranger, la technologie blockchain ouvre des perspectives très intéressantes en matière de fiabilité du vote et pourrait contribuer à rénover notre système démocratique en renforçant la confiance des citoyens.

Dans le cadre de mes fonctions au sein du Gouvernement, j'ai donc considéré que le rôle des pouvoirs publics était d'encourager le potentiel de la blockchain en favorisant le développement d'acteurs français et européens – afin de développer nos propres standards dans ce domaine nouveau plutôt que de les subir de l'extérieur – tout en restant vigilants pour s'assurer de la sécurisation de cette technologie encore très récente.

Le Gouvernement français a donc été pionnier en Europe dans la reconnaissance légale de la blockchain pour certains types de transactions. Les PME peuvent désormais émettre des « minibons », des instruments de dettes transmissibles dont l'échange pourra reposer sur des chaînes de blocs. En outre, le droit sera adapté au cours de l'année 2017 afin d'autoriser l'émission et la transmission des titres financiers non cotés en utilisant la blockchain. Le Programme d'investissements d'avenir, dans son volet « Grands défis » (PIA3), qui prévoit l'encouragement aux technologies de demain comme l'intelligence artificielle, peut également être mobilisé pour financer des projets liés à la blockchain.

Pour autant, nous sommes encore en phase d'apprentissage quant au potentiel comme aux risques possibles liés à la généralisation de la blockchain. D'une part, l'absence de structure de gouvernance centralisée, qui est le cœur de l'intérêt de cette technologie, permet une meilleure résilience en cas de faille d'un réseau et supprime les lourdeurs et les coûts dus à la centralisation. D'autre part, ces mêmes caractéristiques peuvent générer de nouveaux défis sécuritaires, non prévus par les concepteurs initiaux de la blockchain : ainsi, alors même que l'avantage de la blockchain est précisément l'automatisation des processus et l'absence de biais humain, toute intervention *a posteriori*, par exemple pour résoudre une erreur de code informatique, pourrait fragiliser ou invalider l'ensemble d'une chaîne de décisions et surtout remettrait en cause la philosophie initiale de la blockchain, dont l'intérêt est d'être une technologie neutre reposant sur l'automatisation des processus.

Enfin, alors que la blockchain ouvre des perspectives intéressantes en matière d'économies d'énergie, la puissance de calcul considérable aujourd'hui nécessaire pour réaliser les chaînes de bloc a un impact environnemental encore trop élevé.

Ces questions ne doivent pas nous freiner, mais au contraire nous encourager à y répondre par l'innovation. Allier vigilance et confiance dans l'avenir : c'est tout l'enjeu du progressisme, cet optimisme de cœur et de raison.

Axelle Lemaire,
ancienne sécrétaire d'État au Numérique
et à l'Innovation.

PROLOGUE

Retour vers le futur post-blockchain

7 heures : mon réveil sonne, communique par Internet avec la machine à café connectée qui se lance. La quantité de café en réserve diminue dangereusement, la machine commande donc automatiquement sur OpenBazaar[*1], l'Amazon de la blockchain, de nouveaux paquets d'arabica torréfié (un système similaire a été développé par IBM pour une machine à laver Samsung, capable de commander sa lessive). Elle utilise pour cela un « contrat intelligent » (*smart contract*) hébergé sur la blockchain Ethereum : un programme qui m'assure que la commande sera toujours réalisée selon les mêmes conditions, fixées par le contrat. Je traîne un peu et suis en retard, je commande donc un taxi sur mon smartphone, avec l'application Arcade City, le logiciel blockchain d'une coopérative de chauffeurs. Sauf qu'il n'y a plus de chauffeur : seulement des véhicules autonomes dont les propriétaires partagent l'utilisation. Je rentre dans ce véhicule de grand luxe (pourquoi se refuser ce petit plaisir imaginaire ?), qui est évidemment 100 % électrique. Arrivé au feu, le véhicule, à l'arrêt, se recharge en interagissant avec une borne placée sous l'asphalte (système en projet chez Slock.it). Il continue son chemin, mais croise malheureusement une voiture pilotée par un humain à la conduite imprévisible : c'est l'accident ! Rien de grave, mais la carrosserie est endommagée. Ma voiture transmet directement toutes les informations nécessaires à mon assurance automatique, qui me reverse immédiatement le dédommagement qui m'est dû, selon les conditions écrites dans le *smart contract* qui nous lie (de tels systèmes sont en projet chez Axa, IBM et Allianz). J'arrive finalement au travail plus tard que prévu : aucune importance car je n'ai plus de chef. J'ai réservé une place dans un espace de coworking pour la journée. Sur un site dédié, je consulte une liste de missions que je peux accomplir aujourd'hui : je découvre un projet enthousiasmant d'ouvrage collectif sur la blockchain – il s'agit d'écrire une contribution de quelques pages sur l'histoire de cette technologie qui a changé le monde. Ça me plaît, j'ai les compétences nécessaires. Je m'inscris et signe un contrat électronique, livre en fin de journée le texte demandé, et suis payé une fois le document accepté, le lendemain. J'ai ainsi rejoint, le temps d'une journée, une maison d'édition éphémère fondée sur la réalisation de ce seul projet, en y apportant mes compétences sur la tâche où ma valeur ajoutée est la plus

grande (suivant le modèle développé aujourd'hui par OpenOrg.co). Je rentre à la maison à pied, pour me libérer un peu de la technologie, mais c'est une erreur : j'attrape froid. Je prends rendez-vous chez le médecin, qui dispose de toutes mes données médicales en ligne : avec moi, il est le seul à y avoir accès. Toute intrusion dans mes données, dont l'ADN numérique est enregistré sur la blockchain, m'est signalée (comme cela se fait déjà en Estonie). Le remboursement de la consultation est instantané et automatique. À la pharmacie, je paie en Bitcoins en scannant le « QR code » (l'équivalent d'un code-barres) de la facture (avec une application comme celle de Paymium) : c'est immédiat, sans frais, et là encore, le remboursement suit dans la foulée. Le système fonctionne très bien, je suis décidément ravi de la manière dont l'État est géré. Cela tombe bien, car les élections ont lieu aujourd'hui. Une fois chez moi, j'allume mon ordinateur, me rends sur le site du bureau de vote en ligne, j'insère ma carte d'identité électronique (comme il en existe en Estonie) et vote sur la blockchain pour le Président sortant (le système est anonyme et sécurisé, comme celui développé par la start-up Belem). Ma grand-mère, qui pense toujours à l'avenir de ses petits-enfants, m'a transmis la moitié de son bulletin : elle vote de son côté avec une demi-voix et me délègue l'autre moitié, dont je dispose librement (selon les principes de « démocratie liquide » soutenus par la fondation Democracy Earth). À l'issue de cette longue journée, je vais me coucher. J'éteins les lumières. Je n'étais pas là aujourd'hui et j'ai donc peu utilisé d'électricité : le surplus d'énergie produite par les panneaux solaires fixés sur le toit de ma maison est automatiquement revendu aux maisons voisines, dans notre microréseau intelligent (de tels *smart grids* existent dans le quartier de Brooklyn à New York, ou dans celui de la Confluence à Lyon).

---

*1. Toutes les applications citées dans ce prologue imaginaire sont, elles, bien réelles, déjà opérationnelles ou en cours de développement.

INTRODUCTION

La seconde révolution d'Internet

« Ça ne marchera jamais ! » En assénant de telles affirmations, avec l'aplomb cynique de ceux qui en ont vu d'autres, de célèbres capitaines d'industrie sont joliment passés à côté de l'histoire. Le producteur Pascal Nègre, longtemps patron français d'Universal Music, avait déclaré lors d'une convention, en 2001 : « Internet, on s'en fout, ça ne marchera jamais[1] ! » Autre visionnaire malheureux, l'ancien PDG de Microsoft, Steve Ballmer, éclata de rire quand un journaliste du quotidien américain *USA Today* l'interrogea, en 2007, sur l'intérêt que le public portait au premier iPhone d'Apple, qui s'apprêtait à être commercialisé : « Il n'y a aucune chance que l'iPhone prenne une part de marché significative, aucune chance[2] », lâcha-t-il, confiant. Neuf ans plus tard, à l'été 2016, il s'en était écoulé plus d'un milliard, ce qui fait de l'iPhone l'un des produits de consommation les plus vendus de tous les temps. Rétrospectivement, ces erreurs paraissent grossières. Pascal Nègre comme Steve Ballmer avaient pourtant de bonnes raisons d'être méfiants. Leur erreur commune aura été de raisonner au présent, comme si les limites techniques, les cadres légaux, les habitudes de consommation et les services proposés allaient rester les mêmes. Mais tout a changé. Et la révolution a bien eu lieu.

De même que l'essor d'Internet, depuis le début des années 1990, a transformé radicalement notre quotidien, une nouvelle technologie promet aujourd'hui de bouleverser la société, l'économie, la politique, avec autant d'ampleur, et de nous faire à nouveau changer d'époque. Son nom ? La *blockchain*. Comme il y a vingt ans le mot « Internet », ce terme technique anglais nous semble obscur aujourd'hui, mais nous paraîtra naturel demain. De quoi s'agit-il exactement ? Avant tout, d'une technologie qui permet de faire des transactions en ligne sans intermédiaire. De façon plus complète, elle peut être définie comme un registre de transactions numériques, décentralisé au sein de tous les ordinateurs des membres du réseau, que chacun d'entre eux peut consulter, valider et compléter avec ses propres transactions, en suivant des règles cryptographiques qui garantissent que seules des informations authentiques sont ajoutées.

Comme Internet, son fonctionnement technique est un peu complexe à appréhender. Mais qui, à part les informaticiens, sait comment marchent les protocoles TCP/IP, par lesquels nous transférons les données sur le Net, ou http, grâce auquel nous naviguons en ligne ? Nul ne peut pourtant en ignorer ses enjeux, car les usages de cette nouvelle technologie nous concerneront tous. Le Web et le courrier électronique ont permis aux individus d'échanger de l'information directement, partout dans le monde et gratuitement. La blockchain nous offre la possibilité, pour la première fois, d'utiliser le Net pour transférer de l'argent de façon sécurisée, en pair à pair – c'est-à-dire de commercer en ligne sans tiers de confiance. Lorsque nous achetons un objet sur une boutique de e-commerce, l'argent passe par le site, par Visa, Mastercard ou encore Paypal, et *in fine* par votre banque, pour aboutir sur le compte du vendeur. Avec la blockchain, la somme glisse directement de l'acheteur au vendeur, comme de l'argent liquide, sans que personne au milieu ne serve de garant ni ne capte de commission. Plus besoin de banque, de compagnie de carte de crédit ni de site de e-commerce pour certifier un échange : la blockchain est conçue pour garantir son bon déroulement, sans qu'aucun intermédiaire ne soit rémunéré pour authentifier la transaction. En plus de cette fonctionnalité puissante, la blockchain offre deux autres usages majeurs. Elle permet d'enregistrer de l'information de manière immuable : des actes administratifs, des titres de propriété ou encore des diplômes peuvent y être inscrits sans pouvoir être modifiés par la suite, ce qui offre une garantie d'authenticité que fournissaient jusqu'ici les notaires. Enfin, la blockchain donne la possibilité d'héberger des programmes qui automatiseront les communications et transactions entre les milliards d'objets connectés du monde entier (les *smart contracts*).

Une révolution économique

Comme Internet, la blockchain, s'appuyant sur ces trois grandes propriétés, s'annonce comme une profonde révolution économique, au service du consommateur. Nous pourrons bénéficier de produits et de services moins chers, fournis directement par leurs producteurs, avec autant de fiabilité qu'avant, mais plus de transparence : louer un appartement à son propriétaire sans payer de commission à Airbnb, commander un véhicule avec chauffeur sans enrichir Uber, transférer de l'argent au bout du monde pour un coût dérisoire, récompenser directement nos artistes préférés au lieu de passer par l'App Store, acheter de l'électricité au panneau solaire de notre voisin… Les applications sont innombrables. De la finance à l'assurance, du e-commerce à la culture, de l'énergie aux objets connectés en passant par la santé, tous les secteurs sont concernés. Son immense potentiel fait consensus : dans un article publié dans *La Tribune*, Gilles Babinet, représentant du numérique pour la France auprès de la Commission européenne, estime que « parler de révolution ne semble pas exagéré[3] ». Pour le scientifique Joël de Rosnay, elle va « nous permettre de court-circuiter les intermédiaires dans les services, les banques et les assurances ou encore l'immobilier, et de reprendre du pouvoir[4] ». Aux États-Unis, Marc Andreessen, le créateur du premier navigateur Internet Mosaic, fondateur de Netscape et désormais investisseur réputé dans la Silicon Valley, faisait dès janvier 2014 du Bitcoin et de son système de blockchain une révolution

informatique égale aux deux grandes précédentes auxquelles il avait assisté : « l'ordinateur personnel en 1975, Internet en 1993[5] ». L'éloge de la blockchain vient aussi des milieux financiers. Le dimanche 2 octobre, Jean-Claude Trichet, l'ancien président de la Banque centrale européenne (BCE), invité de l'émission *Questions politiques* sur France Inter, affirmait ainsi : « La blockchain est […] une invention géniale, parce qu'elle repose sur une décentralisation complète de l'enregistrement des transactions. Au lieu d'avoir un système central qui enregistre et qui contrôle tout, on est en présence d'une technologie très impressionnante, qu'on a un peu de mal à pénétrer. […] Mais ça marche[6]. » Le patron du marché boursier américain Nasdaq, l'Américain Bob Greifeld, y voit lui tout simplement « la plus grande opportunité imaginable de la décennie à venir[7] ».

En s'appuyant sur la blockchain, des start-up, aux États-Unis, au Royaume-Uni, en Suisse, en Allemagne, en Israël, en Chine mais aussi en France, espèrent faire irruption sur des marchés dominés par des acteurs bien installés et les concurrencer avec des services moins chers (comme Abra le fait avec Western Union, dans le domaine du paiement transfrontalier). Des milliers d'applications sont en développement, bien que peu soient encore commercialisées. Pour les grands groupes, c'est une menace. Avertis des ravages qu'avait causés Internet pour les entreprises qui ne s'y étaient pas adaptées (adieu Kodak), les banques (Goldman Sachs, Santander, Crédit agricole…), les géants de l'informatique (Microsoft, IBM), ceux de l'énergie ou de l'immobilier (RWE, Engie, Bouygues Immobilier), planchent tous sur le sujet. C'est aussi, pour ceux qui tireront leur épingle du jeu, une opportunité de baisser leurs coûts pour gagner en profitabilité et en compétitivité. Tous ou presque y réfléchissent, forment leurs salariés, assistent à des conférences et tentent d'anticiper la manière dont la blockchain va les concerner. Invité à l'université d'été du Medef, fin août 2016, Gilles Babinet racontait ainsi : « Ça intéresse tout le monde au Medef, mais les gens n'y comprennent rien. Ils ont l'impression qu'il faut développer des blockchains. Mais les blockchains ont un modèle économique qui ressemble à l'*open source* [les logiciels dont le code est public]. Les gens se disent : "Je vais faire du pognon avec l'*open source*", mais c'est compliqué. Quand vous êtes un fabricant de Nesquik, faire de la blockchain, c'est pas évident. » Les industries les plus numérisées et celles qui ont recours au plus grand nombre d'intermédiaires dans la gestion de leur flux financiers sont les plus immédiatement concernées : la finance, l'assurance, l'énergie, mais aussi la musique, par exemple. Les industriels également peuvent y trouver un grand intérêt, pour l'automatisation de leur production et la gestion de leurs flux logistiques.

Les plus audacieux, ou plus directement menacés, ont déjà pris l'initiative. C'est le cas de nombreuses banques : un consortium international, R3, réunit ainsi plus de 50 institutions financières majeures, dont Barclays, Crédit Suisse, Société générale ou BNP Paribas, pour développer une blockchain commune, qui serait privée, contrairement aux blockchains Bitcoin ou Ethereum. Les assureurs sont aussi en pointe, comme Axa, qui a investi, début 2016, dans la start-up canadienne Blockstream, lorsque celle-ci a levé 55 millions de dollars (48 millions d'euros). Enfin, les géants informatiques, tels Microsoft et IBM, n'ont pas l'intention de se laisser distancer et développent des projets, notamment dans le domaine des objets connectés. Microsoft s'est même rapproché d'Ethereum, par l'intermédiaire de sa fondation qui promeut cette blockchain au grand potentiel. « Microsoft a été le

principal sponsor de notre conférence annuelle de développeurs, DevCon2, à Shanghai[8] », indique ainsi Ming Chan, la directrice de la Fondation Ethereum. « Nous avons aussi été approchés par de nombreux PDG et directeurs techniques, dans les secteurs du transport aérien, de l'énergie, de la logistique ou encore de l'industrie », ajoute-t-elle. Tous surveillent de près les projets menés par les développeurs qui codent sur Ethereum et n'hésiteront sans doute pas à racheter la première start-up qui les menacera trop frontalement.

Une révolution sociale et politique

Comme Internet, la blockchain promet aussi un profond bouleversement social et politique. Révolution sociale, elle va permettre l'essor de nouvelles organisations, décentralisées et éphémères : des coopératives sans chef, constituées de travailleurs indépendants choisissant une tâche pour laquelle ils sont qualifiés, rassemblés temporairement pour réaliser un projet commun, selon des conditions contractuelles automatisées. Les grandes entreprises au management vertical vont devoir se réinventer. Révolution politique, la blockchain pourra garantir un vote électronique fiable, sans triche possible. Aujourd'hui, le vote électronique, centralisé dans des serveurs, est vulnérable aux attaques des pirates ou aux falsifications de celui qui maîtrise le centre de données. Grâce à la décentralisation des informations et aux techniques cryptographiques de la blockchain, ce ne sera plus le cas. La sécurisation des consultations en ligne offrira de nouvelles manières d'inviter les citoyens à donner leur avis sur les décisions de la cité, afin de bâtir des démocraties plus fidèles à leurs aspirations. L'État, enfin, pourra renoncer à la paperasse et faire fonctionner son administration entièrement en ligne, avec efficacité et transparence, en assurant la sécurité des données des citoyens, à l'image de ce qui se pratique non pas dans le futur, mais à 2 600 km de chez nous, en Estonie.

De plus en plus d'hommes politiques en sont conscients. Dans son initiative sur la technologie et l'innovation, l'ex-candidate démocrate à la présidence des États-Unis, Hillary Clinton, citait la blockchain parmi « la prochaine génération de révolutions technologiques[9] » sur lesquelles les innovateurs américains devaient se positionner en leaders, avec les véhicules autonomes et l'apprentissage automatique des machines (*machine learning*). En France, un premier colloque, réunissant députés et acteurs du secteur, a été organisé à l'Assemblée nationale le 24 mars 2016 (*Blockchain, disruption et opportunités*). Il a été suivi, le 4 octobre 2016, par le premier « Forum parlementaire de la blockchain » : une demi-douzaine de parlementaires de gauche et de droite y ont échangé avec des entrepreneurs et experts du domaine, devant un amphithéâtre de 500 personnes plus que comble, à la maison de la Chimie, à Paris. « La blockchain est-elle aussi révolutionnaire qu'Internet ? Oui, j'en ai l'intuition[10] », a déclaré en préambule Jean Launay, député PS du Lot. Présente également, la socialiste Corinne Erhel, députée des Côtes-d'Armor, partage la même conviction : « Je considère que c'est une des innovations ou des révolutions parmi les plus importantes actuellement[11]. » Pour Laure de La Raudière, députée Les Républicains d'Eure-et-Loir, « trois technologies arrivent en même temps et

sont très disruptives de nos fonctionnements. La première, c'est Internet […]. La deuxième, c'est le Big Data et les algorithmes d'intelligence artificielle […]. La troisième, c'est la blockchain qui permet d'authentifier les transactions, donc de créer de la confiance. Les conséquences de ces trois technologies sur notre société sont colossales[12]. »

Une révolution de la décentralisation

Que ce soit dans ses applications économiques, sociales ou politiques, la blockchain est l'outil d'une vaste révolution de la décentralisation. Elle promet de retirer le pouvoir aux intermédiaires (qu'il s'agisse des banques, de compagnies énergétiques, des géants du Net ou de l'État) et de le redistribuer aux individus : au consommateur, au travailleur ou au citoyen. « Il s'agit avant tout de décentralisation[13] », confirme Bill Barhydt, le PDG d'Abra, une application de transfert d'argent à l'étranger sur la blockchain. « La possibilité de faire des contrats automatiques sur Internet est très puissante et conduira à toutes sortes de nouvelles applications financières, sur des activités sur lesquelles les banques sont très lentes et gagnent beaucoup d'argent. La décentralisation pourra aussi s'appliquer aux cadastres, pour l'enregistrement de titres de propriété immobilière. Et finalement, à l'Internet des objets. Quel registre pourrait gérer les communications de milliards d'objets connectés ? La blockchain, qui élimine le besoin d'une autorité centrale pour coordonner tout cela », assure-t-il. Comme l'écrivent les auteurs d'un rapport publié par le cabinet de conseil Capgemini, « il est vite devenu clair que la technologie qui permet des transactions remarquablement sûres et peu coûteuses sur le réseau Bitcoin pouvait changer complètement la donne pour tous les services financiers – tout comme dans beaucoup d'autres industries[14]. » Par sa transparence (elle est consultable et vérifiable par tous), par son immutabilité et son irréfutabilité (ce qui y est écrit fait consensus entre les membres et ne peut être changé), « l'architecture de la blockchain fait disparaître le besoin d'un intermédiaire central pour garantir la confiance, bouleversant les modèles actuels de centralisation des données et coupant ainsi de manière drastique le modèle de paiement et de coût », résume le rapport.

Nous sommes encore au tout début de l'aventure. À ce stade, la blockchain est une gigantesque promesse : tout reste possible. Personne n'a capturé cette invention, tout le monde peut s'en emparer et transformer le monde selon ses convictions. À l'aune de cette technologie, des futurs radicalement différents peuvent être imaginés. D'un côté du spectre, une utopie libertarienne[*1]. Les individus y ont repris le pouvoir : ils commercent entre eux sans tutelle, leurs rapports sont régulés par des contrats enregistrés dans la blockchain, ils travaillent pour leur compte, les entreprises ont disparu au profit de groupes de projets passagers, l'État est réduit au minimum, la démocratie électronique (directe ou déléguée selon les thèmes par chaque citoyen) garantit que les aspirations de chacun sont prises en compte. À l'opposé, un monde au contrôle renforcé, dans lequel l'esprit libertarien de la blockchain a été subverti : tous les grands intermédiaires (banques, géants des réseaux sociaux et du cloud, États) ont créé leurs propres blockchains, faussement décentralisées et sur lesquelles ils gardent en réalité le contrôle,

comme avant, à ceci près que le système leur permet de faire des économies et, si besoin, de retracer les transactions passées par chacun, la transparence laissant place à la surveillance. Entre ces deux visions extrêmes, qui ne sont souhaitables ni l'une ni l'autre pour ceux qui apprécient à la fois la liberté et l'appartenance à une communauté capable de solidarité, tout un nuancier de possibles existe, dont celui d'un monde où la coopération est favorisée par les applications de la blockchain, où l'État fonctionne de manière transparente et efficace, où la démocratie est participative et où les entreprises, en compétition les unes avec les autres, ne captent pas plus de valeur que n'en méritent leurs services.

---

*1. Une philosophie politique et économique, assez répandue aux États-Unis, qui fait de la liberté individuelle une fin et un moyen. Favorable à la liberté maximale du marché et à un rôle minimal de l'État, elle se distingue de la philosophie libertaire par son attachement à la protection de la propriété privée (que les libertaires voudraient abolir).

PRÉAMBULE

Une brève histoire de la blockchain

L'histoire de la blockchain est pour le moins étonnante. Comment le Bitcoin, la première monnaie virtuelle pair à pair, une invention informatique *open source* à l'esprit libertarien revendiqué visant à court-circuiter les banques, a-t-il pu donner naissance à l'incroyable phénomène blockchain qui agite tous les milieux d'affaires du monde ?

Et Satoshi créa la blockchain

L'aventure commence le 1er novembre 2008. Sous le pseudonyme de Satoshi Nakamoto, une personne, qui n'a toujours pas été identifiée aujourd'hui, publie un message dans une liste de diffusion de spécialistes de la cryptographie (« The Cryptography Mailing List »), avec pour objet « Bitcoin P2P e-cash paper[1] ». Dans des termes très factuels, elle y résume son projet : « J'ai travaillé sur un nouveau système de cash électronique pair à pair, sans tiers de confiance. » Satoshi énumère ses principales caractéristiques. D'abord, « la double dépense est rendue impossible au sein d'un réseau pair à pair. Pas d'émetteur de monnaie ni d'autre tiers de confiance ». C'est un exploit inédit. Jusqu'alors, les experts considéraient qu'il était impossible de créer un système de paiement pair à pair (d'ordinateur à ordinateur) sans tiers de confiance (sans banque par exemple), en raison du problème appelé « double dépense ». Sur Internet, l'information est copiée quand elle est transférée (ainsi conservons-nous une version de nos e-mails envoyés par exemple). Avec de l'argent, il ne peut pas en être de même : un montant envoyé par un réseau électronique ne peut pas être gardé, il ne doit pouvoir être dépensé qu'une seule fois. Sans quoi l'argent, copiable à l'infini, n'aurait plus de valeur… C'est pourquoi les tiers de confiance étaient jusqu'ici nécessaires. Deuxième caractéristique : « Les participants peuvent être anonymes. » En réalité, ils opèrent sous un pseudonyme, qui correspond à une suite de chiffres et de

lettres. Enfin, dernière grande propriété : « De nouvelles pièces sont émises par un système de preuve de travail de style hashcash. » Ce point un peu technique, sur lequel nous reviendrons plus en détail dans la partie suivante, signifie que les nouveaux Bitcoins sont émis progressivement non pas par une banque centrale, comme dans le système financier traditionnel, mais par la validation successive des opérations selon une méthode cryptographique, « la preuve de travail », qui mobilise les ressources des ordinateurs du réseau pour sécuriser les transactions. Satoshi indique également un lien vers son article de recherche (*white paper*), qui détaille le système Bitcoin[2].

L'invention est de taille. « Satoshi Nakamoto a proposé pour la première fois une architecture permettant d'opérer ce transfert de valeur. On passe de la copie de l'information au transfert de valeur, en évitant le problème de la double dépense[3] », confirme Philippe Dewost, directeur adjoint de la Caisse des dépôts et consignations (CDC) en charge de l'économie numérique. Sur Internet, traditionnellement, la banque opère et garantit la transaction. Mais grâce au système proposé par le mystérieux Satoshi Nakamoto, le transfert de monnaie sous forme électronique entre les membres d'un réseau peut avoir lieu avec la certitude que l'argent n'est dépensé qu'une fois, sans aucune tierce partie. Sa solution est simple : tous les participants doivent connaître et approuver l'historique de tous les paiements effectués par chaque membre du réseau. Ainsi peut-on être certain que celui qui envoie un Bitcoin à un autre le possède bien lors de l'envoi, et ne le possède plus après. Pour rendre cela possible, il suggère d'inscrire toutes les transactions à mesure qu'elles ont lieu dans une chaîne de blocs. Chaque bloc est validé, au fur et à mesure, par un système cryptographique complexe (la preuve de travail) : ce dernier assure que chaque membre a une chance de valider le bloc, qu'il est coûteux et difficile de gagner plusieurs fois de suite le droit d'effectuer cette validation, et que tous les membres du réseau peuvent vérifier l'authenticité des informations contenues dans chaque bloc avant de valider le suivant. L'ensemble constitue une chaîne de blocs publique réputée infalsifiable, que l'on appellera, quelques années plus tard, la blockchain. Dans une série de messages, Satoshi Nakamoto répond à toutes les objections formulées par ses pairs cryptographes. Son système ne paraît pas avoir de faille (sauf dans le cas improbable où la majorité de la puissance du réseau est détenue par un membre malveillant). Le 9 janvier 2009, il publie donc un nouveau message sur la même liste de diffusion : « Annonce de la première émission de Bitcoin, un nouveau système de cash électronique qui utilise un réseau pair à pair pour éviter la double dépense. C'est complètement décentralisé, sans serveur ni autorité centrale[4]. » Le mot est suivi d'un lien de téléchargement. Première monnaie électronique pair à pair de l'histoire et première blockchain du monde, le Bitcoin est né. Satoshi Nakamoto apparaît très confiant dans le succès de son invention : « Je serais surpris si, d'ici dix ans, nous n'utilisions pas la monnaie électronique d'une manière ou d'une autre […]. Les applications sont innombrables, dès lors que l'on a la possibilité de payer quelques centimes à un site Internet aussi facilement que l'on introduit une pièce de monnaie dans une distributeur automatique[5]. » Il réalise le vieux rêve de la monnaie d'Internet, qui hantait de longue date les chercheurs en informatique mais aussi les économistes. Dès 1999, le prix Nobel d'économie Milton Friedman avait prédit l'avènement inévitable du Bitcoin : « Ce qui manque [à Internet], mais qui sera bientôt développé, c'est un cash électronique fiable. Une méthode qui permette, quand vous achetez sur Internet, de transférer

des fonds de A à B, sans que A connaisse B ni que B connaisse A[6]. » Milton Friedman est mort le 16 novembre 2006, deux avant que sa prédiction ne soit réalisée.

Un esprit originel libertarien

Dans les rares messages que Satoshi Nakamoto a laissés, il ne s'est guère montré bavard. Ses réponses sont presque toutes d'ordre technique, à l'exception de quelques commentaires sporadiques qui confirment l'esprit libertarien du projet, c'est-à-dire désireux de retirer le pouvoir aux puissances installées – en particulier les banques et les États – pour le rendre aux individus. Moins d'une semaine après la publication de son *white paper*, le 7 novembre 2008, l'un de ses interlocuteurs réagit ainsi : « Vous ne trouverez pas de solution à des problèmes politiques dans la cryptographie. » Satoshi nuance : « Oui, mais nous pouvons gagner une bataille majeure […] et conquérir un nouveau territoire de liberté pour plusieurs années. Les gouvernements savent couper les têtes de réseaux centralisés comme Napster[*1], mais les réseaux authentiquement pair à pair comme Gnutella et Tor[*2] semblent tenir bon[7]. » Sur Bitcoin, il n'y a en effet pas de serveur à couper, qui permettrait de fermer ce système dispersé chez ses utilisateurs. De façon plus explicite encore, Satoshi confirme ses intentions politiques lors d'un message posté le 14 novembre 2008 : « C'est très attirant du point de vue libertarien si nous pouvons l'expliquer correctement. Je suis meilleur avec le code qu'avec les mots toutefois[8]. » Quand il lance véritablement le réseau, début janvier 2009, il se permet une petite fantaisie qui donne sa coloration au projet. L'Europe est alors en pleine crise financière. Dans le tout premier bloc créé (*genesis block*), Satoshi inscrit une suite de chiffres et de lettres qui correspond à la traduction cryptographique d'une courte phrase : « *Times 03/Jan/2009 Chancellor on brink of second bailout for banks*. » C'est la une du quotidien britannique *The Times* daté du 3 janvier, qui titre : « Le ministre des Finances britannique au bord d'un second plan de sauvetage pour les banques. » Pour Pierre Noizat, l'un des meilleurs experts français du sujet, fondateur de la start-up Paymium qui fait office de banque de Bitcoins, « mettre un titre de journal dans un *genesis block*, ça permet de dater précisément le lancement. Mais ce titre du *Times* n'a peut-être pas été choisi au hasard en effet. Il y a cette volonté d'être un contre-pouvoir vis-à-vis des banques ». Deux ans plus tard, le 12 décembre 2010, Satoshi publie un ultime message sur le forum Bitcointalk, puis disparaît. Depuis, une douzaine de développeurs ont été soupçonnés de se cacher sous ce pseudonyme, sans que jamais aucune preuve satisfaisante n'en soit apportée. Le créateur du Bitcoin s'est évaporé, pour sa propre sécurité sans doute. « L'histoire des cryptomonnaies est funeste. Arthur Budovsky, le créateur de Liberty Reserve [une monnaie électronique centralisée, créée en 2006], dort en prison[9] », rappelle Adrian Sauzade, fondateur de la start-up d'assurance blockchain Czam. Hal Finney, le cryptographe américain connu pour avoir reçu la première transaction en Bitcoin de la part de Satoshi lui-même, a été harcelé dans la dernière année de sa vie par un hacker qui voulait lui extorquer 1 000 Bitcoins (l'équivalent de 400 000 dollars à l'époque)[10]. Pas étonnant que Satoshi Nakamoto, dont la

rumeur dit qu'il posséderait 1 million de Bitcoins (évalués à 828 millions de dollars au 14 janvier 2017, soit 777 millions d'euros), ait tenu à rester discret.

Un essor rapide et sulfureux

L'évaporation de son créateur n'a pas empêché le succès rapide du Bitcoin. « Les échanges ont commencé en 2009, à un taux de 0,0007 dollar pour un Bitcoin. En février 2011, le Bitcoin a atteint la parité avec le dollar. En novembre 2013, sa valeur a connu un pic de 1 242 dollars[11] », indiquaient deux experts du Fonds monétaire international (FMI), Hunter Monroe et Andreas Adriano, dans un article paru en juin 2016 dans la revue trimestrielle du fonds, *Finance et Développement*. Il a ensuite chuté, avant de remonter progressivement durant l'année 2016, puis de flamber début 2017, atteignant un nouveau pic à 1 184 dollars le 5 janvier, suivi d'une brusque rechute et d'une stablisation, le 14 janvier 2017, autour de 828 dollars (777 euros environ). Le Bitcoin est une monnaie très volatile… Mais les tout premiers investisseurs ont fait une excellente affaire. Au cours du 14 janvier 2017, la capitalisation du Bitcoin, c'est-à-dire la valeur de tous les Bitcoins en circulation, atteint 13,3 milliards de dollars (12,5 milliards d'euros). L'utilisation de la monnaie virtuelle (ou cryptomonnaie) n'est donc plus du tout marginale, d'autant qu'en parallèle du Bitcoin, une multitude d'autres devises numériques, fondées sur autant de nouvelles blockchains, ont été créées. Plus de 700 sont recensées sur le site CoinMarketCap (gare à celles qui n'y sont pas, ce sont souvent des arnaques). Le Bitcoin reste aujourd'hui de très loin la première d'entre elles. La capitalisation de la seconde, Ethereum, n'atteignait, à la même date, que 849 millions de dollars, soit 797 millions d'euros.

Durant les premières années, le Bitcoin n'a pas séduit que des gens bien intentionnés, ce qui lui a conféré une réputation de monnaie spéculative et sulfureuse, dont il a encore du mal à se défaire aujourd'hui. « Tandis que l'envolée du taux de change a déclenché une sorte de ruée vers l'or, le relatif anonymat du Bitcoin et la facilité d'y faire des échanges ont attiré les dealers de drogues et autres criminels, ce qui a entraîné une lourde répression en 2013 et 2014, qui a conduit quelques entrepreneurs pionniers en prison[12] », analysent Andreas Adriano et Hunter Monroe. Le Bitcoin reste ainsi associé à l'affaire Silk Road : un marché noir de produits illicites (drogues et armes en particulier), sur le Dark Web, l'Internet caché, où les transactions étaient opérées dans cette cryptomonnaie. Depuis la fermeture de Silk Road par le FBI, en octobre 2013, l'activité en Bitcoin s'est largement régularisée, confirme un article du quotidien *Les Échos*, qui relaie les estimations de la start-up américaine Chainalysis, spécialisée dans l'analyse de la blockchain : « L'économie informelle et illicite, autour de 6 % des volumes, est aujourd'hui largement devancée par l'activité financière et spéculative sur les bourses du Bitcoin, qui représente les trois quarts de l'activité mondiale[13]. » La situation n'a donc plus rien à voir avec celle de début 2013, quand « la moitié des transactions réalisées à l'aide du Bitcoin servaient à des activités illégales ». Ce changement est dû à la démocratisation progressive du Bitcoin, mais aussi à la surveillance dont le réseau peut faire l'objet par les services de police. Il n'est en effet pas véritablement

anonyme, mais plutôt « pseudonyme » : chacun y opère aux yeux de tous sous un nom d'emprunt (plus exactement une suite de chiffres et lettres appelée clé publique), dont il est possible de retracer l'historique. C'est pourquoi Marc Andreessen s'exclamait dans le *New York Times* : « Je voudrais répondre aux critiques de ceux pour qui le Bitcoin est un paradis de la mauvaise conduite, des criminels et des terroristes, où on peut transférer de l'argent impunément sous couvert d'anonymat. C'est un mythe […]. Comme l'e-mail, qui est aisément traçable, le Bitcoin fonctionne sous pseudonyme, il n'est pas anonyme. De plus, chaque transaction sur le réseau est tracée et inscrite pour toujours dans la blockchain Bitcoin, un registre permanent, visible de tous. Finalement, le Bitcoin est beaucoup plus facile à suivre pour les forces de l'ordre que le cash, l'or ou les diamants[14]. »

Une reconnaissance tardive sous un nouveau nom : la blockchain

Peu à peu, un glissement sémantique s'opère : créateurs de start-up, financiers et grandes entreprises réalisent que le véritable potentiel du Bitcoin et de ses avatars ne réside pas dans les cryptomonnaies – un terme qui effraie le grand public – mais dans leurs réseaux décentralisés : les blockchains. L'année 2015 marque un tournant. En mars, une vedette de Wall Street, Blythe Masters, ancienne de la banque JP Morgan célèbre pour avoir inventé les CDS (*credit default swap*, des instruments financiers controversés, associés à la crise bancaire de 2008), est nommée PDG d'une start-up blockchain, Digital Asset Holdings. Influente auprès du milieu financier, elle vante les mérites de cette technologie dans les médias et les conférences : « Le marché pour les applications financières blockchain se mesurera au final en milliers de milliards de dollars[15], » lance-t-elle en juin 2015, à la conférence *Exponential Finance*, à New York. De quoi éveiller la curiosité de l'assemblée. Le 30 juillet 2015, une nouvelle blockchain très prometteuse est lancée : Ethereum. Imaginée par un jeune génie de l'informatique canadien d'origine russe, Vitalik Buterin, 19 ans à l'époque, celle-ci reprend les principes de la blockchain Bitcoin (un réseau public décentralisé de blocs de transactions), en ajoutant la possibilité d'inscrire des programmes dans la blockchain, appelés *smart contracts*. Débarrassée de l'idéologie libertarienne du Bitcoin, elle promet d'innombrables applications (dans l'assurance, l'énergie et les objets connectés en particulier) et apparaît beaucoup plus amicale au monde des affaires. Trois mois plus tard, le 31 octobre 2015, la technologie blockchain fait la une de l'hebdomadaire britannique *The Economist*. Bible des milieux économiques, le magazine réussit l'exploit de résumer en trois mots sur sa couverture tout l'intérêt de la blockchain : « *The trust machine* » (« La machine à fabriquer de la confiance »). C'est un déclic. Adoubée par *The Economist*, la blockchain fait parler d'elle dans les couloirs des grandes entreprises, qui redoutent de rater le nouvel Internet. Le phénomène se répand dans les salons professionnels et les journaux, offrant une légitimité tardive mais bienvenue aux start-up pionnières qui s'étaient lancées sur la blockchain Bitcoin. « Avant le début de l'année 2015, on était radioactifs[16] », témoigne Manuel Valente, directeur de la Maison du Bitcoin, un comptoir d'achat de cryptomonnaies doublé d'un institut de formation, installé dans le Sentier, à Paris. « Après, on a commencé à devenir intéressants pour les

entreprises, notamment les banques, auprès de qui on fait maintenant des formations. On ne parle pas Bitcoin, on parle blockchain. Le Bitcoin, c'est mal, la blockchain, c'est bien », commente-t-il en souriant. « Avant, tu disais Bitcoin à un banquier, impossible d'ouvrir un compte », se souvient Adrian Sauzade, qui a connu la mésaventure avec sa start-up Czam. « Aujourd'hui, tu dis blockchain, la banque te dit oui. » Partout dans le monde, les investisseurs suivent cette même logique. Au premier trimestre 2016, 84 % des fonds de capital-risque levés dans le secteur l'ont été par des start-up offrant des services fondés sur des blockchains, contre 16 % pour celles travaillant sur des cryptomonnaies, rapporte une étude de l'agence de notation Moody's : « Un plus grand nombre de nouvelles sociétés purement blockchain ont été lancées et celles fondées sur des cryptomonnaies ont pivoté vers des solutions blockchain plus larges[17] », commentent les auteurs. Au total, selon ce même rapport, entre 2012 et mi-juillet 2016, 149 start-up Bitcoin et blockchain ont levé pas moins de 1,2 milliard de dollars de capital-risque. La révolution est en marche.

---

*1. Le premier grand site de téléchargement de musique illégal.

*2. Respectivement un système de transfert de fichier pair à pair et un logiciel permettant d'utiliser Internet de manière anonyme.

PREMIÈRE PARTIE

COMMENT FONCTIONNE UNE BLOCKCHAIN ?

CHAPITRE PREMIER

Qu’est-ce qu’une blockchain ?

Soyons rassurés : de même que la plupart d’entre nous conduisent une voiture sans connaître les secrets du moteur à explosion, branchent des appareils à des prises en ayant tout oublié des notions de circuits électriques enseignées au collège et consultent leurs e-mails dix fois par jour sans même connaître l’existence des protocoles de messagerie, il sera tout à fait possible d’utiliser des services sur la blockchain en ignorant tout de son fonctionnement. En revanche, il est préférable d’en comprendre dès maintenant les enjeux. Les avantages – un moindre coût de transaction, une grande praticité et rapidité d’exécution, une sécurisation des données et une transparence renforcée – suffiront à convaincre les moins curieux. Il est même probable que la plupart des applications blockchain que nous utiliserons ne mettront pas en avant cette technologie complexe, mais seulement ce qu’elle apporte. C’est le cas du site de transfert d’argent transfrontalier Abra, par exemple, qui ne promeut pas du tout son utilisation du réseau Bitcoin, mais seulement la possibilité qu’il offre d’envoyer des fonds instantanément, de manière sécurisée et à peu de frais, à l’autre bout du monde. « Si l’on veut que la blockchain ait du succès, il faut concevoir des produits qui ont des bénéfices directs pour les usagers, qui ne sauront même pas qu’ils utilisent la blockchain. Tant que ça marche, on ne se pose pas la question de comment », considère Stephan Tual, le fondateur de Slock.it, une des start-up les plus connues du secteur, qui associe blockchain et objets connectés. « Mon but ultime, c’est qu’un jour ma mère aille charger sa voiture autonome quelque part, et que je lui dise, là, tu utilises un de mes produits. Et elle aura enfin compris ce que je fais », confie-t-il. Pas besoin d’attendre, elle peut le faire dès aujourd’hui. Car en réalité, ce n’est pas si compliqué.

Définition

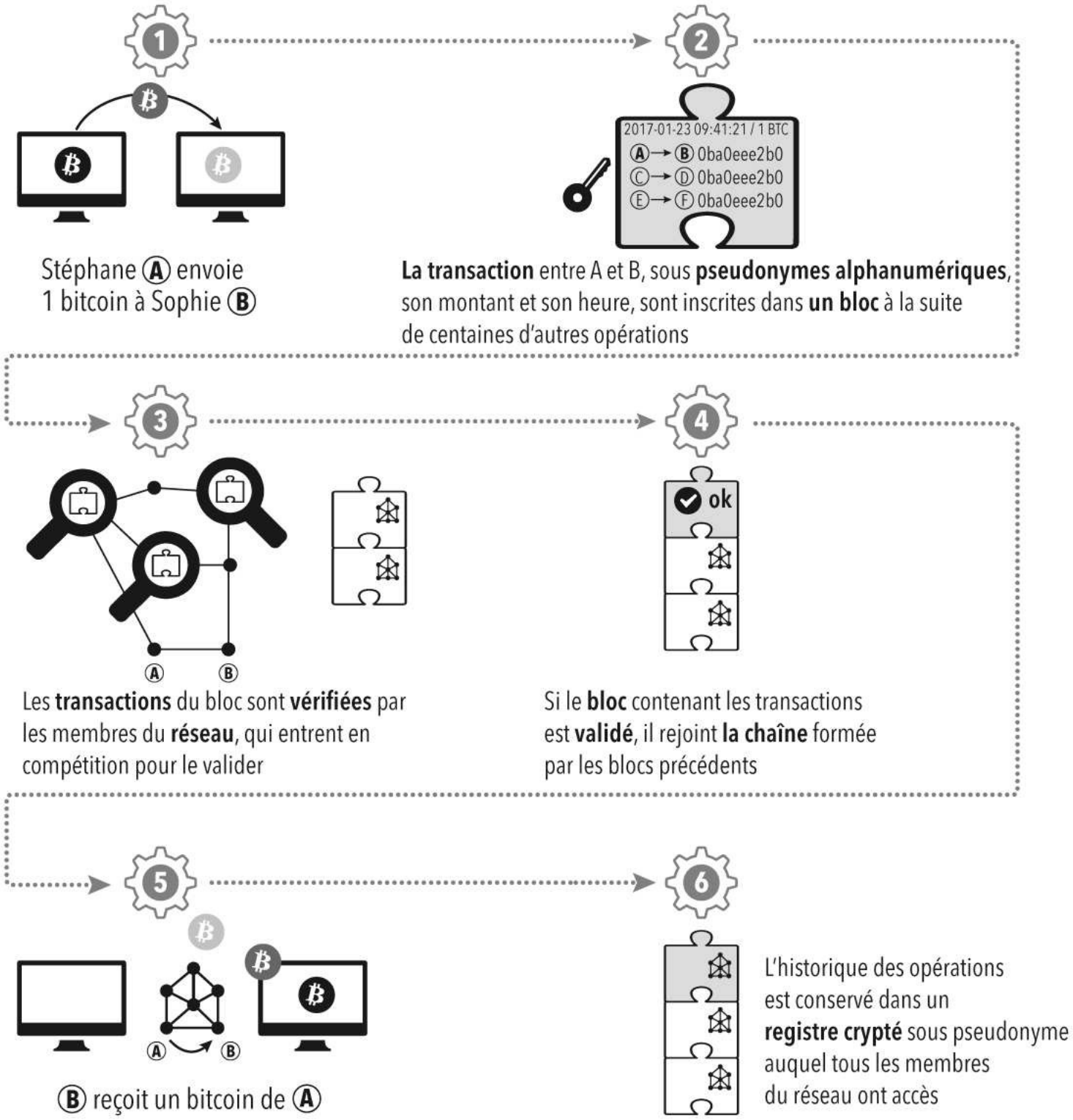
Il y a deux façons de définir la blockchain. La manière simple consiste à la décrire par ses usages : la blockchain est une manière sécurisée de faire et d'enregistrer des transactions numériques sans intermédiaire. « Quand j'ai expliqué la blockchain à ma sœur, je lui ai dit que c'était pour moi avant tout un système qui permet de notariser[*1] des transactions, grâce à un algorithme qui assume le rôle joué normalement par un tiers de confiance (comme un notaire avec un cadastre ou un banquier avec un livre comptable)[1] », raconte Emmanuel Méthivier, patron du CA Store, la start-up en charge de l'innovation au Crédit agricole. Mais le vrai défi consiste à décrire la blockchain non par ce qu'elle fait, mais par ce qu'elle est. « Si je devais expliquer la blockchain à ma grand-mère », tente François Dorléans, directeur des opérations de Stratumn, « je lui dirais que c'est un grand registre, un grand livre, qui est distribué : c'est-à-dire que tout le monde possède ce même registre. À chaque fois qu'une personne y écrit quelque chose, l'information est répliquée sur tous les exemplaires du registre de toutes les autres personnes. Comme on veut garantir l'authenticité de ce que chacun écrit dedans, un mécanisme de consensus entre les utilisateurs assure que tout le monde s'accorde sur les données inscrites, et que si quelqu'un marque quelque chose de faux, cela ne sera écrit que dans son livre et pas dans tous les livres ». Grâce à ce mécanisme, qui donne à chaque membre du réseau la possibilité de vérifier tout l'historique de toutes les transactions, il est possible d'être sûr que celui qui envoie une certaine somme la possède bien (c'est inscrit dans la blockchain) et que cet argent n'est envoyé qu'une seule fois (et n'est donc pas dupliqué). C'est ce qu'explique, en des termes plus techniques mais plus précis, un rapport du cabinet d'audit Deloitte, qui donne la définition suivante des blockchains publiques (les plus utilisées, certaines dites privées ayant un fonctionnement différent, fermé, avec parfois une autorité centrale) : « Une blockchain publique est un registre digital de transactions, distribué sur l'ensemble du réseau et dont les copies sont identiques sur l'ordinateur de chaque membre du réseau. Aucune autorité centrale ne régit ce réseau. N'importe quel acteur du réseau peut visualiser les entrées du registre et enregistrer de nouvelles transactions. Les désaccords sont réglés par consensus d'une majorité des membres du réseau. Les transactions sont regroupées en blocs qui sont ensuite reliés les uns aux autres, formant ainsi une chaîne de blocs, d'où le nom de blockchain. Les données contenues dans les blocs sont cryptées et ne peuvent pas être "craquées", en théorie. Ainsi, une fois enregistrées dans la blockchain, les informations ne peuvent plus être effacées. Par essence, la blockchain contient un enregistrement précis, horodaté et vérifiable de chaque transaction[2]. »

Si l'on lie les deux définitions de la blockchain, par les usages et par le fonctionnement, on peut ainsi considérer qu'elle est un registre où les transactions numériques réalisées par les membres d'un réseau sont enregistrées les unes après les autres, dont tous les utilisateurs possèdent chacun un exemplaire au contenu identique, qui fait consensus entre eux et ne peut être changé. Ce mode de fonctionnement leur apporte la confiance nécessaire à la réalisation de nouvelles transactions, sans qu'une tierce partie ne soit nécessaire pour les superviser.

La blockchain pas à pas

Pour comprendre vraiment comment fonctionne une blockchain, le plus simple est de suivre l'itinéraire d'une transaction (même si l'immense majorité de ceux qui utiliseront un service sur la blockchain passeront par des intermédiaires qui leur simplifieront la tâche et se chargeront de l'enregistrement de l'opération sur le réseau). Prenons le cas d'une opération réalisée sur la plus ancienne et la plus commune des blockchains, Bitcoin, qui a servi de modèle à l'ensemble de celles qui ont suivi.

1) Stéphane souhaite envoyer 1 Bitcoin à Sophie (soit 777 euros au cours du 14 janvier 2017). Sur le réseau Bitcoin, chacun possède une adresse publique, appelée « clé publique » (l'équivalent d'un RIB) : une suite d'environ 34 caractères contenant des chiffres et des lettres en minuscules ou majuscules (par exemple : 13o7TCoNWbaqYp9g89w1gHrZ7GvvKftgQm pour l'un et 16Xgsii16x4icN7yjQgXX648Lf4LxvDy7j pour l'autre).


1
2
2017-01-23 09:41:21 / 1 BTC
Ⓐ → Ⓑ 0ba0eee2b0
Ⓒ → Ⓓ 0ba0eee2b0
Ⓔ → Ⓕ 0ba0eee2b0
Stéphane Ⓐ envoie 1 bitcoin à Sophie Ⓑ
La transaction entre A et B, sous pseudonymes alphanumériques, son montant et son heure, sont inscrites dans un bloc à la suite de centaines d'autres opérations
3
4
ok
Ⓐ
Ⓑ
Les transactions du bloc sont vérifiées par les membres du réseau, qui entrent en compétition pour le valider
Si le bloc contenant les transactions est validé, il rejoint la chaîne formée par les blocs précédents
5
6
Ⓑ reçoit un bitcoin de Ⓐ
L'historique des opérations est conservé dans un registre crypté sous pseudonyme auquel tous les membres du réseau ont accès

2) Stéphane signe la transaction avec sa clé privée : une autre suite de chiffres et de lettres, cette fois-ci confidentielle (c'est l'équivalent numérique de la clé de votre coffre-fort, que vous n'avez donc intérêt ni à donner ni à perdre), qui autorise le versement de l'argent (points 1 et 2 correspondant à l'étape 1 du schéma).

3) La transaction est alors écrite dans la blockchain. Elle est entrée, à la suite d'autres transactions, dans ce qui est appelé un bloc (une grappe de plusieurs centaines, voire milliers, de transactions).

Pour chaque transaction, différentes informations apparaissent et seront donc consultables par tous les membres du réseau :

– les clés publiques de Stéphane et de Sophie : les transactions ne sont donc pas anonymes, mais réalisées sous les pseudonymes que constituent ces clés publiques ;

– le nombre de Bitcoins transférés de Stéphane à Sophie : 1 ;

– l'heure précise, à la seconde près, et la date à laquelle l'opération a eu lieu (2017-01-23 09 : 41 : 21).

4) Chaque bloc, en plus de toutes ces transactions, contient un résumé cryptographique du bloc précédent : un nombre, qui correspond à l'unique résultat possible que l'on obtient quand on entre les informations du bloc précédent dans une fonction appelée SHA256 (appelé le hash, soit le résultat d'un algorithme de hashing). Cela permet de noter dans chaque bloc l'ADN cryptographique du bloc précédent. Ainsi, si un pirate veut modifier a posteriori les informations d'un bloc, il devra corriger tous les blocs qui suivent, et ce sur chaque exemplaire de la blockchain hébergé par chaque ordinateur du réseau (ce qui est quasiment impossible). Par ce système, les blocs sont donc enchaînés les uns aux autres (d'où le nom « blockchain » – points 3 et 4 correspondant à l'étape 2 du schéma).

5) Les membres du réseau qui le souhaitent vont alors entrer en compétition pour valider le bloc. On les appelle les « mineurs ». Ils y sont incités par une récompense : celui qui aura le privilège d'effectuer cette validation gagnera automatiquement 12,5 nouveaux Bitcoins (soit environ 9 712 euros au 14 janvier 2017), qui seront générés pour l'occasion par le système. Pour gagner ce droit, tous les participants vont vérifier la véracité des informations contenues dans toutes les transactions du bloc : est-ce que Stéphane possède bien 1 Bitcoin au vu de toutes les transactions qu'il a déjà réalisées ? N'utilise-t-il bien ce Bitcoin qu'une seule fois ? Est-ce que les autres transactions sont également justes ? Mais ils vont aussi devoir résoudre un problème mathématique complexe, en utilisant les capacités de calcul de leur ordinateur (c'est le système de « preuve de travail », ou *proof of work*, détaillé plus bas). Chaque ordinateur va tester des solutions jusqu'à trouver la bonne. Le premier à réussir pourra valider le bloc et gagner la récompense. Le système a été conçu pour qu'une solution soit trouvée au bout de 10 minutes en moyenne (ce qui impose un léger délai à la sécurisation de la transaction – point correspondant à l'étape 3 du schéma).

6) Le bloc est alors validé. Il est ajouté à la blockchain qui est mise à jour sur les ordinateurs de chaque participant (point correspondant à l'étape 4 du schéma).

7) Les participants n'acceptent ce nouveau bloc que si les transactions qu'il contient sont valides (si l'argent de chaque transactionneur n'y est bien dépensé qu'une seule fois). Si le bloc est valide, ils expriment leur accord en travaillant sur le bloc suivant selon le même processus, et y inscrivant le hash du bloc validé. C'est pourquoi on parle de système de consensus.

8) Sophie a désormais reçu le Bitcoin envoyé par Stéphane. En récompense du travail fourni, le mineur reçoit une certaine quantité de cryptomonnaie créée pour l'occasion (12,5 Bitcoins à ce jour, mais ce rendement décroît au fil du temps – points 7 et 8 correspondant aux étapes 5 et 6 du schéma).

Ce système présente bien les propriétés promises :

– *la décentralisation* : les données ne sont pas toutes regroupées dans le serveur d'un intermédiaire central, mais au contraire « distribuées », c'est-à-dire hébergées chez chaque participant ;

– *la transparence* : toutes les transactions sont publiques et vérifiables par tous, ce qui va permettre à chacun de s'assurer que chaque participant possède bien les Bitcoins qu'il dépense et qu'il ne les dépense qu'une fois ;

– *le consensus* : la blockchain correspond à un historique de transactions sur lequel tout le monde s'accorde. Comme l'explique le fondateur de Paymium, Pierre Noizat, « ce consensus sur le séquencement des transactions permet de résoudre le problème dit de la "double dépense" : un Bitcoin dépensé dans une transaction ne peut pas être dépensé une deuxième fois dans une transaction qui serait diffusée ultérieurement sur le réseau. La deuxième transaction serait rejetée par le réseau[3] » ;

– *la sécurité* : le système cryptographique de validation garantit qu'il est quasiment impossible de réécrire une transaction une fois son bloc validé (personne n'a réussi à le faire depuis la création du Bitcoin).

La blockchain (ici celle du Bitcoin) remplit bien sa promesse de rendre possibles des transactions numériques sécurisées en pair à pair (donc sans intermédiaire). Sur un point toutefois, l'engagement n'est qu'à moitié tenu : les participants n'opèrent pas sans aucune identification, comme le voudrait un système véritablement anonyme (quand nous payons avec du liquide par exemple), mais sous un pseudonyme associant lettres et chiffres. Un enquêteur tenace pourrait éventuellement réussir un jour à relier celui-ci à une identité réelle, auquel cas il disposerait de l'ensemble de l'historique de transactions de celle-ci.

---

*1. Certifier.

CHAPITRE 2

Les mécanismes du consensus

La validation des transactions constitue le point critique d'une blockchain : comme un bloc validé ne peut pas être réécrit, il faut être certain que les informations gravées dans la blockchain sont authentiques, et donc que celui qui valide fait honnêtement son travail. Pour cela, il existe différents mécanismes de consensus (comme celui de la preuve de travail), qui ont pour ambition de garantir la fiabilité de la chaîne de blocs, même dans le cas où certains membres du réseau seraient mal intentionnés. Ces mécanismes sont des solutions à une question informatique ancienne, appelée « le problème des généraux byzantins », et présentée pour la première fois en 1982 par trois chercheurs américains, Leslie Lamport, Robert Shostak et Marshall Pease. Ils la résument ainsi : « Des systèmes informatiques fiables doivent pouvoir gérer des composants qui dysfonctionnent et donnent des informations contradictoires à différentes parties du système. Cette situation peut être représentée de manière abstraite par un groupe de généraux de l'armée byzantine qui camperaient avec leurs troupes autour d'une ville ennemie. Communiquant uniquement par l'intermédiaire de messagers, ils doivent se mettre d'accord sur un plan de bataille commun. Toutefois, un ou plusieurs d'entre eux pourraient être des traîtres qui tenteront de semer la confusion chez les autres. Le problème est de trouver un algorithme qui assure que les généraux loyaux trouveront un accord[1]. » Comme l'expliquent les auteurs d'un rapport du cabinet KPMG, « il y a une analogie directe avec les monnaies numériques, la propriété de biens et le transfert de valeur quand il n'y a pas d'autorité centrale pour vérifier ces biens et ces transactions. Dans les registres distribués [comme les blockchains], les différents nœuds [ordinateurs] participant sont comme les généraux[2] », relèvent Sigrid Seibold et George Samman. En conclusion du Forum parlementaire de la blockchain, Axelle Lemaire, alors secrétaire d'État au Numérique et à l'Innovation, résumait la solution : « La réponse, c'est de développer une technologie qui assure que quand un message malveillant est envoyé, une règle de consensus l'étouffe[3]. » Reste à trouver la règle de consensus. Et c'est là que ça se complique.

Il existe deux principales méthodes : l'une, fiable, mais lente et coûteuse en énergie, est la preuve de travail (souvent désignée par sa version anglaise, *proof of work*) ; la seconde, plus pratique, moins énergivore mais à la fiabilité plus contestée, est appelée en anglais *proof of stake* (elle peut être traduite par « preuve d'enjeu », « de possession » ou « d'intérêt »).

Une première solution : la preuve de travail (*proof of work*)

Cyril Grunspan, le responsable du département d'ingénierie financière de l'École supérieure d'ingénieurs Léonard-de-Vinci (l'Esilv), nous présente ce système : « Le principal problème, c'est d'éviter les tentatives de double dépense : j'ai de l'argent, j'achète un téléphone portable en ligne, mais dans le dos du vendeur, je fais une autre acquisition avec le même argent (par exemple des places de spectacle). C'est beaucoup plus compliqué à gérer dans un réseau décentralisé que s'il y avait une personne centrale qui validait les transactions. Si je peux moi-même écrire le fameux registre qui enregistre les transactions correctes, je peux escroquer les gens. Il faut absolument éviter cela. Comment ? La solution proposée est assez ingénieuse. Il faut à la fois inciter les personnes honnêtes à prendre part à la maintenance du réseau[*1] et rendre difficile le travail d'éventuels escrocs. Comment inciter les personnes honnêtes ? En les rémunérant. Celui qui enregistre une page de transactions et l'ajoute au registre (que l'on appelle un "mineur") va gagner de l'argent (12,5 Bitcoins sur le réseau éponyme). Le système est conçu de manière à ce que tout le monde ait une chance réelle de gagner, pour que ce ne soit pas la loi du plus fort, de l'ordinateur le plus puissant, qui s'applique. Pour cela, il leur est demandé d'effectuer une "preuve de travail" : pour écrire un nouveau bloc, il faudra non seulement recopier sur le registre des transactions réelles, nouvelles et légales, mais il faudra en plus résoudre un petit problème mathématique propre à chaque machine et de difficulté équivalente, conçu pour être surmonté en 10 minutes à peu près. C'est un problème dit d'inversion[*2], qui utilise une fonction de hashage : une fonction dans laquelle on peut entrer n'importe quoi (un fichier, une lettre, n'importe quel document numérique) et qui produit toujours une suite alphanumérique de taille fixe. Dans le cas du Bitcoin, la fonction utilisée s'appelle SHA256 (elle est publique, *open source*). Vous y entrez un document numérique, il en ressort une suite alphanumérique qui a l'air complètement aléatoire, mais qui est comme l'ADN unique du document hashé. Deux documents hashés avec cette fonction obtiendront toujours deux résultats différents[4]. » Pour résoudre ce problème, chaque ordinateur participant va tester des solutions jusqu'à trouver la bonne : il y a ainsi une part de chance (chacun a la possibilité de trouver la solution en premier) et une part de probabilité (plus l'ordinateur d'un mineur est puissant et calcule vite, plus celui-ci a de chance d'être le premier à résoudre le problème, valider le bloc et gagner la récompense). Le résultat est difficile à trouver, mais facile à vérifier. « Comme un sudoku[5] », s'amuse Alain Brégy, cofondateur de la start-up Aedeus. Sur la blockchain Bitcoin, « la difficulté du problème est recalculée tous les 2 016 blocs, avec l'objectif de maintenir un temps moyen de 10 minutes pour

découvrir un nouveau bloc. À cette vitesse idéale, 2 016 blocs seront découverts toutes les deux semaines[6] », précisent les chercheurs Karl J. O'Dwyer et David Malone, du Hamilton Institute, à l'université nationale d'Irlande à Maynooth.

Cette méthode rend le travail d'escrocs quasiment impossible. « Imaginons que l'escroc achète le téléphone portable », poursuit Cyril Grunspan. « Le vendeur interroge la blockchain et constate que la transaction fait bien partie de la chaîne de blocs et que plusieurs blocs (disons 6 ou 7) se sont ajoutés à celui qui contient la transaction. Il se dit que la transaction est bonne et envoie donc le téléphone. » Pour l'escroc, la seule façon de truander est alors, une fois le téléphone envoyé, de réécrire la blockchain en faisant disparaître la transaction par laquelle il envoie son Bitcoin contre un téléphone en la remplaçant par une transaction où il envoie le même Bitcoin contre des places de spectacle. Mais pour cela, il devrait produire une chaîne de blocs plus longue que la chaîne officielle, où l'achat du téléphone portable serait effacé au profit de l'achat des places de spectacles. « Pour modifier un bloc passé, confirme Satoshi Nakamoto dans son *white paper*, l'attaquant devrait refaire la preuve de travail du bloc et de tous ceux qui suivent et ensuite rattraper et dépasser le travail fait par tous les nœuds[*3] honnêtes[7]. » Dans le cas de notre escroc, « comme le vendeur de téléphone portable a attendu 6 ou 7 certifications avant de faire son envoi, cela signifie que l'escroc doit produire, plus rapidement que l'ensemble de la communauté, une chaîne de blocs plus longue que la chaîne officielle, avec 6 ou 7 blocs de retard. C'est comme battre un champion du monde de 100 mètres avec 50 mètres de retard. C'est peine perdue », conclut Cyril Grunspan. À une exception près toutefois : « Si l'escroc détient plus que la moitié de la puissance du réseau, alors il pourra écrire plus vite que l'ensemble des membres, mais c'est impossible aujourd'hui [tant le réseau est grand]. »

L'intérêt d'un système si lourd de validation est donc de rendre très compliquée et très coûteuse, voire quasi impossible, la réécriture de la chaîne de blocs. Imaginons même qu'un participant ait suffisamment de ressources pour s'approprier plus de la moitié de la puissance du réseau. Il n'aurait en réalité pas intérêt à le faire, car alors plus personne n'aurait confiance dans la blockchain : les Bitcoins (ou toute autre monnaie numérique dans cette situation) perdraient toute leur valeur. « Si un mineur ou un groupe de mineur non identifié contrôle le réseau, celui-ci devient sujet à une réécriture de l'historique et, de fait, perd à la fois sa sécurité et son utilité. Dans ce cas, les mineurs décident de réduire leur puissance de calcul, ou de se séparer pour éviter cette dangereuse centralisation qui réduirait considérablement la valeur des Bitcoins[8] », explique Pierre Noizat.

Une deuxième solution : la preuve d'enjeu (*proof of stake*)

La preuve de travail a un gros inconvénient : elle mobilise la puissance de calcul de tous les ordinateurs qui entrent en compétition pour valider un bloc et consomme donc énormément d'énergie. Une autre méthode a été imaginée en 2012 pour contourner ce désavantage : la preuve d'enjeu, plus connue

sous son appellation anglaise, *proof of stake*. Selon Sigrid Seibold et George Samman, du cabinet KPMG, celle-ci consiste à « créer un mécanisme qui punit les nœuds qui ne suivent pas le protocole de consensus. Les participants doivent miser un montant prédéfini d'actifs numériques (des Bitcoins) sur le résultat du consensus. Si ce résultat n'a pas lieu, les nœuds malveillants [ceux qui avaient parié contre le consensus majoritaire] perdent leur mise[9]. » En résumé, ceux qui tentent de tricher en validant un bloc qui ne devrait pas être validé sont pénalisés financièrement. Dans ce type de système, la probabilité d'être choisi pour miner un bloc (c'est-à-dire valider une série de transactions et gagner la récompense correspondante en cryptomonnaie) dépend de la quantité de cryptomonnaie possédée par le mineur. Si vous possédez 10 % du total, vous avez 10 % de chances d'être choisi. « L'avantage du *proof of stake* par rapport au *proof of work* est que cette méthode demande moins de calculs laborieux. Comme ces calculs sont généralement onéreux, leur réduction diminue le coût du système », indiquent les experts de KPMG. Mise en place pour la première fois avec le Peercoin, un avatar du Bitcoin créé en 2012, cette méthode est utilisée par plusieurs autres cryptomonnaies, comme ShadowCash. La deuxième plus grande blockchain existante derrière Bitcoin, Ethereum, fonctionne pour l'instant en *proof of work*, mais son fondateur, Vitalik Buterin, a annoncé sa volonté de passer à terme à un système de validation *proof of stake*. « Les développeurs Ethereum veulent permettre à des personnes de se présenter comme des validateurs de confiance », explique Simon Polrot, fondateur d'un site d'information dédié à cette blockchain, Ethereum France, et avocat spécialisé dans le droit des nouvelles technologies au cabinet Fieldfisher. « Ces derniers signeraient les transactions et valideraient leur authenticité. Pour s'assurer que ces validateurs sont fiables, ils seraient obligés de mettre en dépôt leurs Ethers (la cryptomonnaie d'Ethereum) pour effectuer ce rôle. S'ils ne valident pas correctement, ils perdent des Ethers. Ce sera la première mise en échelle industrielle de ce principe[10] », indique-t-il.

Ce système possède toutefois des inconvénients, jugés rédhibitoires par certains. Ses détracteurs, comme Pierre Noizat, le considèrent d'abord comme moins sûr. « Le système prête le flanc à une attaque assez simple[11] », écrit-il. « Un fraudeur peut se procurer à moindres frais des clés de signatures obsolètes à partir des premiers blocs de l'historique des transactions. Il aura ainsi les moyens de réécrire l'historique en sa faveur jusqu'au moment présent. S'ils ont vendu leur participation, les anciens signataires n'ont pas vraiment d'incitation à garder leurs clés secrètes et seront prêts à les céder au pirate à vil prix. » Dans un article de recherche publié en janvier 2014, l'économiste Nicolas Houy, du CNRS, a relevé une autre faille du même genre : « Si l'attaque est menée par quelqu'un qui veut de manière crédible anéantir la cryptomonnaie, les agents [les autres membres du réseau] devraient anticiper que leurs coins [la cryptomonnaie] n'ont plus de valeur dès le départ et devraient les vendre à l'assaillant pour presque rien[12]. » Deuxième type de critique : pour Pierre Noizat, l'utilisation du *proof of stake* reviendrait à privatiser la blockchain, normalement censée être une structure distribuée et *open source*. En effet, « la validation des transactions repose sur ceux qui possèdent les coins, de la même façon que les droits de vote au conseil d'administration d'une société anonyme sont détenus par les actionnaires. De mon point de vue, en *proof of stake*, c'est un système propriétaire, privatisé dans les faits par les possesseurs de coins. » Ensuite, Nicolas Houy rappelle que c'est un système qui n'a jamais été testé à

large échelle : les cryptomonnaies comme Peercoin ou Shadowcash ne dépassent pas 15 millions de dollars de capitalisation (contre 849 millions de dollars pour Ethereum et 13,3 milliards de dollars pour Bitcoin, au 14 janvier 2017). Enfin, le chercheur relève un problème de conception même du système : « Si j'ai beaucoup de pièces [d'une cryptomonnaie fonctionnant en *proof of stake*], je vais pouvoir miner et gagner de nouvelles pièces. La valeur d'une pièce est donc à augmenter des pièces qu'elle pourrait engendrer. C'est une distorsion économique[13]. »

D'autres mécanismes de consensus

Au fil des années, de multiples autres systèmes de consensus ont été imaginés. Celui de la blockchain Ripple, troisième la plus utilisée (248 millions de dollars de capitalisation au 14 janvier 2017), repose sur le choix d'un certain nombre de validateurs de confiance qui ne se connaissent pas. Le protocole Raft, lui, élit des leaders au sein du réseau, chargé de répliquer l'information à ceux qui les suivent. Une infinité de systèmes peuvent être imaginés, mais la plupart d'entre eux reposent, *in fine*, sur le choix d'intermédiaires de confiance au sein du réseau (précisément ce que permettait d'éviter le mécanisme de sélection aléatoire du validateur par la preuve de travail). La start-up française Aedeus a ainsi imaginé sa propre méthode : « Je décris notre projet comme un village de machines sociales. Dans ce village, tout le monde ne sait pas tout sur tout. Il suffit de demander à 5 machines ce qu'elles savent sur la machine A et, si elles sont d'accord et trouvent la même chose, alors on considère que la transaction est bonne. Si elles ne tombent pas d'accord, on va demander au voisin. Les machines ne sont pas chacune obligées de détenir toutes les informations. Mais il doit être possible à tout moment de réunir ces informations réparties entre toutes les machines. Cela permet d'avoir des transactions instantanées et moins consommatrices d'énergie[14] », commente le cofondateur, Alain Brégy. Il est probable que, d'ici quelques années, de multiples blockchains dotées chacune de mécanismes de consensus différents coexistent, en fonction des besoins, estiment Sigrid Seibold et George Samman, de KPMG : « Nous croyons que les mécanismes de consensus vont évoluer pour atteindre des besoins spécifiques, qu'il s'agisse d'une application particulière, de possibilités techniques ou d'un environnement réglementaire[15]. »

---

*1. N'importe quel utilisateur peut essayer de valider une transaction.

*2. De type f(x) < y : y est donné par le réseau, il s'agit de trouver x.

*3. Membres.

CHAPITRE 3

Caractéristiques des blockchains

Quelles informations peut-on inscrire dans la blockchain ?

Une fois validées par ces différents mécanismes de consensus, les transactions sont donc enregistrées dans la blockchain. Ces transactions peuvent contenir trois grands types d'informations, qui ouvriront la voie à autant de grands types d'usage. D'abord, elles enregistrent le transfert d'un montant en cryptomonnaie, comme on l'a vu dans le cas de Bitcoin, et rendent ainsi possible les applications de paiements. Mais ce n'est pas tout. La blockchain permet aussi d'enregistrer le hash, c'est-à-dire l'ADN d'un document, dans le message qui accompagne une transaction, comme l'explique le Dr Cécile Monteil, consultante pour la start-up Stratumn, dans un article de *La Tribune* : « La Blockchain offre une fonctionnalité cruciale : intégrer un "message" à chaque transaction, qui fera partie intégrante de celle-ci, bénéficiant donc du même niveau de sécurité. Mais, ce message ne peut contenir que 40 caractères, et 40 caractères, c'est encore moins qu'un tweet ! On ne va donc pas stocker dans la transaction toute l'information qui nous intéresse, et qui est en général très volumineuse, mais seulement une preuve de cette information. Comment ? Choisissez l'information dont vous voulez garder une preuve : un contrat, des photos, une vidéo, un livre, etc. Hachez cette information dans un "hachoir" à Blockchain par un algorithme dédié : le SHA256. Et vous obtiendrez un code unique lié à l'information entrée : un hash, empreinte digitale cryptée de votre document et inférieur à 40 caractères, donc facilement intégré dans ce fameux "message". C'est donc ce hash qui sera stocké sur la Blockchain, et non les informations initiales[1]. »

Enfin, certaines blockchains comme Ethereum permettent d'enregistrer un troisième type de contenu : un *smart contract*, c'est-à-dire un programme informatique, comparable à un contrat, qui versera une somme de cryptomonnaie prédéfinie si une ou plusieurs conditions préétablies sont remplies. Tim Swanson, le directeur de la recherche de R3, un consortium de plus de 50 grandes banques mondiales axé sur l'innovation blockchain, les définit ainsi : « Les *smart contracts* sont des protocoles

informatiques qui facilitent, vérifient, exécutent et font respecter les termes d'un accord commercial[2]. » En accueillant ces trois types d'information (paiement, hash d'un document et *smart contract*), la blockchain offre une quasi-infinité d'applications, du transfert international d'argent à l'enregistrement d'un titre de propriété immobilière en passant par le remboursement automatique d'un sinistre par une assurance.

Les cryptomonnaies

Le site CoinMarketCap recense plus de 700 cryptomonnaies différentes, correspondant à autant de blockchains. Chaque blockchain est en effet associée à une cryptomonnaie (Bitcoin, Ether, Litecoin…) dans laquelle se déroulent les échanges. Pourquoi les transactions n'y ont-elles pas lieu directement en dollars ou en euros ? C'est que créer une blockchain revient à donner naissance à quelque chose qui n'existait pas avant : du « cash électronique pair à pair », ainsi que l'appelle Satoshi Nakamoto dans son *white paper*. En d'autres termes, une unité d'échange que l'on va pouvoir transférer sans tiers de confiance d'un ordinateur à un autre. Un euro ou un dollar, même transféré sur Internet, est aussi un actif physique, stocké dans un compte chez un établissement financier, et créé soit par la Banque centrale (américaine ou européenne le cas échéant), soit par les banques commerciales (quand elles prêtent plus d'argent qu'elles n'en ont en dépôt et font ainsi circuler de la nouvelle monnaie). Personne d'autre n'a le droit de produire des euros ou des dollars. Si l'on souhaite mettre en place un système électronique de transfert de valeur purement pair à pair, sans tiers de confiance, il ne faut pas qu'une autorité centrale ait le contrôle de la monnaie utilisée. Il faut donc un actif *ad hoc*, inventé pour l'occasion, où l'argent fait corps avec le réseau décentralisé : le Bitcoin par exemple. Cette cryptomonnaie est générée, au fil des transactions, par les validations des blocs (à chaque bloc ajouté, un mineur est récompensé pour son travail par une quantité de cryptomonnaie qui s'ajoute à celle en circulation). Tous les Bitcoins existant ont ainsi été générés successivement par le minage des blocs de la chaîne : la validation du tout premier bloc en a créé 50, il y en a aujourd'hui 16,1 millions (au 14 janvier 2017). Si toutes les pièces d'une cryptomonnaie sont créées par le minage des blocs, il est toutefois possible d'acheter (avec des euros, des dollars ou autre) de la cryptomonnaie déjà existante à quelqu'un qui en possède. De multiples intermédiaires (comme Paymium ou La Maison du Bitcoin par exemple) le proposent : ils agissent comme des plateformes de change ou des banques, achètent ou revendent pour vous la monnaie virtuelle en question sur d'autres plateformes spécialisées. Le jeu de l'offre et de la demande sur ces plateformes d'échange permet de donner aux cryptomonnaies une valeur, généralement exprimée en dollars, dans le système économique traditionnel. Celles qui ont un grand nombre d'utilisateurs et dans lesquelles le marché a confiance voient leur cote augmenter : c'est ainsi qu'un Bitcoin valait, au 14 janvier 2017, 828 dollars et un Ether, 9,70 dollars. Les cryptomonnaies sont néanmoins très volatiles : elles font l'objet d'une forte spéculation et leur cours fluctue grandement, en fonction notamment des cyberattaques qui visent les plateformes de change.

Quelles sont les spécificités des différentes blockchains existantes ?

Toutes les blockchains sont des avatars du Bitcoin. Elles en reprennent les grands principes mais changent tel ou tel aspect, pour compenser ce que leurs créateurs estiment être un défaut de leur ancêtre. Pour accélérer l'enregistrement des transactions et diminuer la consommation d'énergie du réseau, certaines modifient leur mécanisme de consensus (Aedeus par exemple). Pour élargir les usages possibles, d'autres, comme Ethereum, adaptent le langage informatique pour rendre possible l'inscription de programmes élaborés (*smart contracts*). Pour garantir plus de confidentialité à leurs clients, quelques-unes (comme celles sur lesquelles les banques travaillent par exemple) renoncent au caractère public de la blockchain et optent pour un réseau fermé : on les appelle alors des blockchains privées (ou de consortium). Enfin, pour gérer les éventuelles erreurs et éviter qu'elles soient fixées pour de bon dans la chaîne de blocs, l'entreprise Accenture a même poussé l'inventivité jusqu'à concevoir ce qui pour beaucoup apparaît comme une contradiction dans les termes : une blockchain révisable, qu'une autorité centrale a la possibilité d'amender après coup. Examinons les spécificités des plus grandes blockchains publiques (Bitcoin et Ethereum), privées (Hyperledger et Corda) et d'une alternative à mi-chemin (les « sidechains »).

La blockchain Bitcoin

Modèle d'origine des blockchains, celle du Bitcoin est publique : n'importe qui peut la télécharger, examiner toutes les transactions (*via* le site blockchain.info par exemple, qui fait défiler tous les blocs validés en direct), devenir un nœud, c'est-à-dire un membre du réseau, et tenter de miner un bloc en utilisant la puissance de calcul de son ordinateur. Elle fonctionne, comme on l'a vu, par un mécanisme de consensus *proof of work*. Ce dernier garantit sa sécurité, qui n'a jamais été compromise depuis sa création[*1]. Les piratages ont visé des plateformes d'échanges mais la blockchain, elle, est restée intacte. Son succès auprès de très nombreux utilisateurs la rend particulièrement solide : « Bitcoin est la blockchain qui a le plus de nœuds, c'est-à-dire de gens qui la stockent. Elle est donc très résiliente, car plus un réseau est petit, plus il est facile à attaquer », relève Louison Dumont, fondateur de Bitproof. Le 20 octobre 2016, le site Bitnodes dénombrait environ 5 160 nœuds en activité (il y a bien plus d'utilisateurs du Bitcoin, mais qui ne conservent pas de copie de la blockchain et ne minent pas de transactions). L'ancienneté du réseau, qui lui permet d'avoir une très longue chaîne de blocs liés les uns aux autres, est un autre gage de sûreté. En contrepartie de cette sécurité, le mécanisme *proof of work* limite la rapidité d'exécution des transactions – un bloc n'est validé que toutes les 10 minutes – et demande, comme on l'a vu, une dépense considérable d'énergie. Le réseau Bitcoin possède deux autres spécificités. D'abord, sa masse monétaire, constituée par tous les Bitcoins créés par la validation des blocs depuis la création, est finie, comme l'a voulu son créateur : « La circulation totale sera de 21 millions de Bitcoins. Ils seront distribués aux nœuds du réseau quand ils feront des blocs, avec un montant divisé par deux tous les 4 ans. Quatre premières années : 10 500 000 Bitcoins. Quatre suivantes :

5 250 000 coins. Quatre suivantes : 2 625 000 coins. Quatre suivantes : 1 312 500 coins[3] », indiquait Satoshi Nakamoto au premier jour du lancement de la cryptomonnaie, le 9 janvier 2009. Cette division par deux s'opère plus précisément tous les 210 000 blocs. Ainsi, un mineur qui validait un bloc gagnait à l'origine 50 Bitcoins, puis à partir du 28 novembre 2012, seulement 25 Bitcoins, et enfin, depuis le 9 juillet 2016, 12,5 Bitcoins. La récompense continuera d'être amputée de moitié avec la même régularité. Pour les amateurs de mathématiques, l'évolution de la quantité de Bitcoins en circulation peut être représentée par une courbe logarithmique qui tend vers 21 millions. Il y avait, le 14 janvier 2017, 16 102 125 Bitcoins en circulation (à 828 dollars l'unité, la capitalisation totale atteignait 13,3 milliards de dollars). Le Bitcoin est, dans une certaine mesure, comparable à l'or : c'est une matière précieuse, qui existe en quantité limitée, dont une partie des stocks n'a pas été mise à jour et doit être minée, ce qui demande un certain investissement en énergie et de la chance. « L'analogie est intéressante[4] », juge l'économiste Nicolas Houy, du CNRS, mais ce dernier pointe quelques petites différences : « D'abord, l'or, contrairement au Bitcoin, a une "utilité d'usage" [il ne sert pas seulement de valeur d'échange] : il faut de l'or pour les composants électroniques et les bijoux. Ensuite, comme le Bitcoin, l'or est produit en quantité limitée, mais l'or disponible est extrait de façon probabiliste : on n'est pas sûr de la quantité qui va sortir. L'empire espagnol a beaucoup souffert de l'arrivée massive d'or d'Amérique du Sud au XV^e^ et XVI^e^ siècle. Avec le Bitcoin, on sait en revanche exactement quand et ce qu'on va miner. Enfin, la dernière différence est énorme : le Bitcoin, c'est un or qui se transfère de Paris à Bangkok en quelques dixièmes de secondes et presque sans frais. Les banques sont nées pour éviter de transporter de l'or ou des métaux précieux sur de grandes distances. Si à la Renaissance, il y avait eu le Bitcoin, il n'y aurait pas eu de banques ! » conclut-il. « Plus sérieusement, c'est plus sûr que l'or, car on ne peut pas se faire voler physiquement quelque chose », souligne l'économiste. On pourrait donc imaginer que le Bitcoin joue un jour, sur les marchés financiers, un rôle de valeur refuge lors de crises monétaires, comme l'or actuellement. Certains l'utilisent déjà ainsi, mais il faut avoir le cœur bien accroché, au vu des évolutions assez erratiques du cours (il est passé de 1 149 dollars le 30 novembre 2013 à 208 dollars en janvier 2015, puis a atteint 1 184 dollars le 5 janvier 2017 avant de retomber à 828 dollars le 14 janvier 2017). La dernière spécificité fondamentale de la blockchain Bitcoin réside dans la simplicité de son code informatique, dont les possibilités sont volontairement limitées. « Le langage utilisé est très rudimentaire, on voit à bout de nez ce qui se passe », commente Cyril Grunspan, de l'Esilv (à condition toutefois d'avoir les compétences d'un développeur informatique : le commun des mortels n'y comprend rien). Cette langue possède une limite fondamentale : elle n'est pas *turing complete*, comme le disent les spécialistes. En d'autres termes, « on ne peut pas faire de boucle, pas de fonctions récursives dessus », précise Cyril Grunspan. Les boucles permettent de répéter des instructions autant de fois qu'on le souhaite sans avoir à les recoder à chaque fois. Ne pas pouvoir faire de boucle, « cela permet de garder la maîtrise ce que l'on fait », insiste Cyril Grunspan. Cela enlève aussi une arme aux hackers malveillants qui voudraient insérer un programme malin dans la blockchain. « La simplicité du Bitcoin réduit le potentiel pour des failles », confirme le jeune développeur Louison Dumont, fondateur de Bitproof. Mais cela limite aussi les usages : les *smart contracts*, ces programmes qui automatisent une relation

contractuelle et permettent le versement d'une somme sous certaines conditions, sont ainsi développés bien plus facilement sur la blockchain Ethereum que sur celle du Bitcoin, comme nous allons le voir.

La blockchain Ethereum : un « ordinateur mondial »

Challenger du Bitcoin, dont elle est largement inspirée, la blockchain Ethereum est celle qui intéresse le plus les milieux d'affaires, qui voient en elle à la fois une version « politiquement correcte » du Bitcoin (sans l'arrière-fond idéologique anarchiste de la cryptomonnaie originelle) et un outil aux possibilités plus larges. Elle est née de l'imagination de Vitalik Buterin, un jeune et très brillant développeur canadien d'origine russe, né le 31 janvier 1994. En 2011, âgé de 17 ans, il se prend de passion pour le Bitcoin et cofonde, en septembre 2011, *Bitcoin Magazine*, une des premières publications spécialisées sur les cryptomonnaies. Deux ans plus tard, il publie un article de recherche intitulé « Une nouvelle génération de plateforme pour les *smart contracts* et les applications décentralisées[5] ». Il y propose la création d'un nouveau réseau, Ethereum, qui permettrait d'exploiter pleinement le potentiel des blockchains grâce à un langage *turing complete*, visant à faciliter la programmation de *smart contracts*. « En décembre 2013, quand il a écrit ce *white paper* à seulement 19 ans, il ne savait pas vraiment ce qui allait suivre. Il l'a envoyé à une vingtaine de personnes qui ont répondu avec enthousiasme et ont soutenu sa vision[6] », raconte Ming Chan, la directrice de la Fondation Ethereum. Le projet se concrétise rapidement autour d'une petite équipe d'experts, qui accompagne Vitalik. En juillet 2014, une prévente de 60 millions d'Ethers (la cryptomonnaie d'Ethereum) est organisée et permet à la fondation de lever 31 591 Bitcoins, l'équivalent à l'époque de 18 millions de dollars. Un an plus tard, le 31 juillet 2015, la blockchain est véritablement lancée : « À ce moment-là, personne ne savait si ce serait un succès », témoigne Ming Chan. C'en fut un. L'Ether, qui vaut encore moins d'un dollar au 31 décembre 2015, voit son cours s'envoler en 2016 pour dépasser les 10 dollars début mars. Le pic de 19,42 dollars est même atteint en juillet 2016, mais un hack fait chuter la devise, qui se maintenait tout de même aux alentours de 8 dollars fin 2016. La personnalité hors du commun du créateur, Vitalik Buterin, dont les portraits commencent à fleurir dans la presse généraliste (en 2016, il a été classé 31e personnalité de moins de 40 ans la plus influente au monde, par le magazine *Fortune*), n'est pas pour rien dans ce succès. « Il est brillant et possède une grande intégrité. Il fait un excellent travail pour diriger ce projet[7] », confirme Joseph Lubin, un des cofondateurs d'Ethereum, ancien financier de Goldman Sachs qui dirige aujourd'hui une start-up d'applications sur Ethereum, Consensys.

Pourquoi le projet de ce petit génie du code a-t-il suscité tant d'enthousiasme ? Sous ses aspects fondamentaux, Ethereum fonctionne comme Bitcoin : le réseau est public et adopte un mécanisme de consensus *proof of work* (bien que le passage en *proof of stake* soit en projet). Mais il apporte diverses améliorations (au détriment de la sécurité, disent ses détracteurs). D'abord, la confirmation des transactions y est nettement plus rapide. « Aujourd'hui, la validation d'un bloc sur Ethereum prend 15 secondes environ, contre 10 minutes sur Bitcoin[8] », indique Simon Polrot, du site Ethereum France. Comme sur Bitcoin, des Ethers sont créés après l'enregistrement d'un bloc (aucune limite n'est toutefois

fixée à leur quantité, contrairement au réseau de Satoshi Nakamoto). Mais la différence fondamentale entre les deux grandes blockchains réside dans le langage de programmation : à l'inverse du Bitcoin, celui d'Ethereum est *turing complete*. « Ça donne la possibilité de réaliser des boucles et de faire des fonctions récursives », précise Cyril Grunspan. Plus concrètement, « cela permet d'écrire des contrats (appelés, dans le style marketing fréquent dans le monde Ethereum, des *smart contracts*) qui sont la description, dans un langage de programmation, des règles qui s'imposent aux parties contractantes. Un prêt d'argent, par exemple, peut se programmer dans un contrat et s'exécuter automatiquement, sans intervention humaine, et donc sans possibilité de triche[9] », écrit le blogueur spécialisé Stéphane Bortzmeyer. « Il existe des cryptomonnaies comme le Bitcoin. Mais imaginez que cette monnaie numérique ne soit plus seulement utilisée comme devise, mais qu'elle intègre un langage de programmation, et qu'avec ce code, vous puissiez créer des programmes, dans une optique de business », explique Ming Chan. Ces *smart contracts* permettent de donner naissance à des applications décentralisées sur la blockchain Ethereum (D-App), dans n'importe quel domaine (énergie, santé, finance, assurance, administration, pari ou encore vote, comme nous le verrons dans la partie suivante). Ces applications sont dites « décentralisées » car elles fonctionnent par un code inscrit dans la blockchain, elle-même hébergée chez chaque nœud du réseau. Ethereum se transforme ainsi en plateforme globale d'applications décentralisées, ce que son fondateur appelle parfois une « machine virtuelle », un « ordinateur mondial » ou même un « ordinateur magique ». Ainsi écrivait-il sur son blog en avril 2105, quelques mois avant le lancement officiel d'Ethereum : « La blockchain est un ordinateur magique qui permet à quiconque d'inscrire un programme en son sein, et de laisser les programmes s'y exécuter seuls, de manière publique avec la possibilité permanente de voir l'état présent et passé de chaque programme, avec une garantie très forte […] que le programme continuera à s'exécuter exactement selon ce que spécifie le protocole dans la blockchain[10]. »

Cette plateforme a vocation à faciliter la vie des développeurs, qui donneront ainsi naissance à tout un nouveau monde d'applications décentralisées. « Cette machine virtuelle met à portée de n'importe quel développeur la possibilité de bâtir des applications décentralisées sophistiquées, aussi facilement qu'une application mobile », s'enthousiasme Joseph Lubin. Ce qui était impossible sur Bitcoin : « Le Bitcoin est excellent pour transmettre et stocker de la valeur, mais affreux pour y écrire des applications », juge ce dernier. Pour son collaborateur John Lilic, conférencier et expert de l'utilisation de la blockchain dans le secteur de l'énergie chez Consensys, « vous pouvez comparer le Bitcoin aux anciens téléphones Blackberry, très sécurisés pour les fonctions de messagerie. Mais ensuite est arrivé l'iPhone, qui était véritablement une plateforme, comme l'est Ethereum pour les applis décentralisées[11] ». Pour les détracteurs d'Ethereum toutefois, la sécurité des transactions y est plus faible que sur Bitcoin. « Il y a eu de vraies dérives, des bugs de programmation qui n'auraient jamais eu lieu sur Bitcoin, car Bitcoin n'est pas *turing complete* », insiste Cyril Grunspan. L'enseignant fait référence au piratage retentissant de TheDAO en juin 2016 : une organisation décentralisée sur Ethereum qui a levé 168 millions de dollars avant de s'en faire détourner près du tiers par l'inscription d'un programme malveillant dans la blockchain. Ce type de hack n'était jamais arrivé sur Bitcoin (des plateformes

d'échanges s'y sont fait pirater mais jamais la blockchain elle-même). Comme l'a prouvé cette affaire, du chemin reste donc encore à parcourir pour l'ambitieux Ethereum, en particulier en termes de sécurisation.

Les blockchains privées

Si formidables que soient les blockchains Bitcoin et Ethereum, elles présentent néanmoins un gros défaut aux yeux de beaucoup d'entreprises : elles sont publiques. Or, même si elles fonctionnent sous pseudonymes (chacun opérant sous le masque d'une suite de chiffres et lettres, la clé publique), il est toujours possible de retracer les mouvements financiers de chaque clé publique. Cette confidentialité très relative est tout à fait insuffisante pour assurer le secret des affaires. Une solution existe, les blockchains privées (ou « de consortium ») : des réseaux fermés, auxquels seuls les membres ont accès, et qu'on ne peut rejoindre sans autorisation (venant des membres ou d'un administrateur désigné par ces derniers). « Les industriels et les banquiers privilégient la mise en place de blockchains de consortium (partagées entre plusieurs entreprises) », indique Nadia Filali, responsable des activités blockchain au sein de la Caisse des dépôts et consignations et copilote de l'initiative Labchain lancée par la CDC pour coordonner l'action d'une vingtaine d'institutions financières françaises. Une étude récente du réseau interbancaire European Financial Management Association (EFMA) et du cabinet Deloitte le confirme : pour 53 % des institutions financières interrogées, c'est la « blockchain privée détenue par un consortium » qui permettra l'adoption à grande échelle de cette technologie (seuls 11 % misent sur la blockchain publique)[12]. La start-up Stratumn, qui développe des applications sur la blockchain pour des entreprises, partage le même sentiment : « Dans le domaine des applications B to B[*2], les clients ne veulent pas utiliser la blockchain Bitcoin, ils nous achètent des blockchains privées, où les données sont échangées dans ces réseaux entre entreprises », confirme le cofondateur, François Dorléans. Ces dernières fonctionnent, pour la plupart, avec un administrateur central, qui distribue les autorisations d'accès (c'est quand elles sont distribuées par plusieurs membres du réseau, plutôt qu'un seul, que l'on parle de « blockchain de consortium »). Beaucoup de grands groupes et d'institutions financières de premier plan misent sur les blockchains privées, ou de consortium, dans lesquelles ils voient un moyen de baisser leurs coûts de transaction et de fonctionnement, tout en conservant la confidentialité requise par leur activité (et parfois même par la réglementation de leur secteur). Deux projets majeurs ont été lancés. Le premier, Hyperledger, a été annoncé fin décembre 2015 par la fondation Linux, et réunit aujourd'hui plus de 85 membres, dont Accenture, Airbus, Fujitsu, JP Morgan, Intel ou encore IBM, qui fut parmi les premiers d'entre eux. « L'objectif est de fédérer tous les efforts de développement des principaux acteurs technologiques et industriels pour créer une blockchain avec permission[*3], qui puisse être utilisée dans les contextes réglementés où nos clients opèrent[13] », explique Luca Comparini, l'expert blockchain d'IBM France. « Le gros enjeu, c'est de préserver la confidentialité de certaines informations », insiste-t-il. Qui sera garant du système ? « Sur un réseau avec permission, il y a un élément de gouvernance centralisé, pour donner des droits d'accès aux nœuds. Cette personne sera désignée en fonction de cas usages (ce ne sera pas forcément IBM, nous ne dirigeons pas Hyperledger). Imaginons que les banquiers

français décident d'utiliser Hyperledger. Ils choisiront qui va gérer ce type de blockchain. Ce pourrait être un régulateur ou la banque de France par exemple », précise Luca Comparini.

L'autre grand projet est mené par le consortium interbancaire R3 (ou R3 CEV), qui a confirmé, en novembre 2016, sa volonté de lever 150 millions de dollars pour mettre au point Corda, que l'entreprise qualifie de « registre distribué pour les services financiers » plutôt que de blockchain. Selon son concepteur, Richard Brown, Corda est « un système où une entreprise pourrait regarder l'ensemble de ses accords avec une contrepartie » et savoir à coup sûr que « ce que je vois est ce que tu vois et que nous savons tous deux que nous voyons la même chose et que cette information est transmise au régulateur » [14]. Ainsi, Corda pourra servir de réseau au sein duquel les banques adhérentes pourraient mener des opérations financières entre elles, en étant certaines que chacune enregistre bien les mêmes mouvements de fonds et que les autorités sectorielles ont les mêmes données sous les yeux. Au caractère fermé de ce réseau, Corda ajoute une garantie de confidentialité. Contrairement aux blockchains classiques, toutes les transactions ne seraient pas copiées sur chaque exemplaire de la chaîne de bloc. « Nous rejetons le principe selon lequel toutes les données seraient copiées auprès de tous les participants, même si elles sont cryptées », précise Richard Brown. Pour Alain Brégy, le fondateur de la start-up Aedeus, « en gros, leur projet est de remplacer Swift », l'actuel réseau interbancaire dans lequel les transferts de fonds, opérations et autres recouvrements sont inscrits, et qui repose sur des bases de données centralisées chez la société Swift, basée en Belgique. Malheureusement, R3 rencontre, depuis l'automne 2016, de sérieuses difficultés : plusieurs membres éminents, comme Goldman Sachs, Morgan Stanley et Santander ont décidé de quitter l'aventure en raison des désaccords avec l'équipe de Corda sur leurs parts respectives dans le capital du consortium.

Certains sont néanmoins sceptiques sur les blockchains privées ou de consortium : « Quel est l'intérêt par rapport à une base de données privée partagée ? » s'interroge ainsi Laurent Benichou, directeur de l'innovation et de la prospective chez Axa. La désintermédiation et la décentralisation promises par la blockchain disparaissent en effet dans de tels systèmes, où un administrateur ou plusieurs membres désignés ont une influence plus grande que les autres sur le fonctionnement du réseau. Quentin de Beauchesne, le fondateur de la start-up française Ledgys, qui conçoit des applications décentralisées, est très méfiant lui aussi : « La blockchain privée n'est pas une bonne idée. J'y vois deux gros points noirs : d'abord, le consensus a lieu dans un réseau fermé. Donc si un hacker externe l'infiltre, il peut le faire tomber. Pire, si un acteur interne décide de modifier les paramètres, il peut devenir impossible de l'arrêter. Ensuite, dans les blockchains publiques, le code est en *open source*, visible, alors que les blockchains privées ne montrent pas leur code en public, donc on ne peut pas être sûr de la sécurité du réseau, on est obligé de faire confiance. » Un des apports majeurs de la blockchain disparaît : il faut à nouveau faire confiance à quelqu'un. « Je crois que les blockchains privées n'ont pas vraiment d'avenir, pour moi l'avenir appartient aux plateformes privées bâties au-dessus de blockchains publiques, des "surcouches", comme ce que nous proposons chez Ledgys », estime Quentin de Beauchesne.

Les « sidechains »

Pour accélérer les transactions ou garantir la confidentialité tout en bénéficiant de la solidité des grandes blockchains publiques, certaines start-up ont développé des « sidechains » : des blockchains parallèles à une blockchain principale (en général Bitcoin). Le rapport du cabinet Deloitte précise leur fonctionnement : « Ce protocole permet de “geler” un certain nombre de Bitcoins de la blockchain Bitcoin et de les faire migrer vers une autre blockchain. Une fois dans la nouvelle blockchain, ces Bitcoins peuvent être transférés selon les règles en vigueur dans le nouvel environnement, par exemple un temps de validation des blocs plus court, un mécanisme de consensus différent, des caractéristiques de programmation plus avancées, etc.[15]. » Dans cette bulle, il est donc possible de moduler les règles pour contourner les désavantages du Bitcoin – la lenteur et l'absence de confidentialité – tout en gardant un lien avec Bitcoin, gage de sécurité et de solidité. Un plus grand volume d'informations peut ainsi être traité au sein d'une blockchain, tout en gardant un lien avec la blockchain principale. Cela permet d'accélérer l'enregistrement d'une transaction. L'entreprise canadienne Blockstream, dans laquelle Axa a investi, est l'une des premières à avoir misé sur ce type de réseau, avec son projet « sidechains », que l'assureur français définit comme « un protocole blockchain capable de mettre en place des réseaux publics et privés pouvant interagir les uns avec les autres, et ainsi d'assurer des transactions agiles et sécurisées ». Pour Laurent Benichou, d'Axa France, « l'idée est de désengorger la blockchain Bitcoin, en mettant des transactions dans des blockchains satellites, qui ont un point de contact avec la blockchain principale Bitcoin. Imaginons que je vende et achète des actions toutes les secondes, elles seront toutes répertoriées dans une blockchain satellite et j'inscrirai seulement à la fin de la journée le montant total des achats et des ventes dans la blockchain principale ». Cela va plus vite et tout le monde ne voit pas le détail des échanges.

Quelle sera la blockchain gagnante ?

Nous sommes à un stade très précoce de développement de la technologie blockchain et la forme que prendra sa démocratisation fait débat. Il existe des puristes du Bitcoin, pour qui c'est la seule blockchain vraiment sécurisée, l'unique capable de porter la révolution de la décentralisation promise. D'autres ne jurent que par Ethereum, qui affiche son ambition de devenir la blockchain globale de référence. Simon Polrot, l'animateur du site Ethereum France, estime que le Bitcoin sera cantonné à la fonction de réserve de valeur, tandis qu'Ethereum aura un rôle bien plus large : « Le Bitcoin n'a pas vocation à être utilisé dans la vie de tous les jours. Ethereum, par son caractère beaucoup plus programmable, pourra plus facilement devenir ce que certains souhaitaient que Bitcoin devienne, une blockchain de référence très souple, qui s'adapte à tous types d'utilisation[16] », parie-t-il. Une troisième voie est possible : celle de la coexistence d'une infinité de blockchains. Il y aurait alors toujours des grandes blockchains publiques : Bitcoin serait utilisé pour le paiement numérique et la notarisation (c'est-à-dire l'enregistrement daté de documents) et Ethereum servirait de plateforme pour d'innombrables applications décentralisées (notamment pour les communications entre objets connectés).

Mais il y aurait aussi de multiples blockchains privées (ou des sidechains), aux modes de fonctionnement adaptés à leurs usages. « C'est tout à fait possible qu'il y ait une, deux ou trois blockchains publiques dominantes, accompagnées d'une foison de blockchains privées ou de sidechains, qui fonctionneraient un peu comme des intranets[17] », estime Claire Balva, la cofondatrice de Blockchain France. Gilles Babinet privilégie aussi ce scénario et ne croit pas au monopole des blockchains publiques : « Vous ne faites pas la même blockchain si vous traitez des bons du Trésor américain par lot d'un million ou si vous faites des objets connectés, car les enjeux de sécurité et de temps réel ne sont pas les mêmes[18] », souligne-t-il. François Dorléans, de Stratumn, croit à la multiplication des blockchains : « Notre vision, c'est que dans 10 ans il y en aura un million, comme il y a aujourd'hui des millions de bases de données[19] », parie-t-il. Tous partagent en tout cas une conviction : le succès à venir de la technologie blockchain, quelle que soit la forme qu'il prendra.

---

*1. Un bug avait toutefois été découvert et vite résolu en août 2010.

*2. D'entreprises à entreprises.

*3. Équivalent d'une blockchain de consortium.

DEUXIÈME PARTIE

QUELLES FUTURES APPLICATIONS ?

La blockchain offre trois grands types de fonctionnalités au potentiel incommensurable : le paiement numérique (qui peut être fait de pair à pair, sans intermédiaire), l'exécution automatique de contrats (grâce aux *smart contracts*, ces logiciels qui déclenchent des versements d'argent sous des conditions prédéfinies) et la notarisation (l'enregistrement et la vérification d'informations datées et sanctuarisées, comme si elles étaient passées entre les mains d'un notaire). De ces trois fonctionnalités, parfois combinées, découlent de véritables révolutions économiques et citoyennes en gestation. La première, la possibilité de faire des transactions en ligne sans intermédiaire, a des impacts sur l'ensemble du secteur financier : banques commerciales et banques centrales, compagnies de cartes de crédit, sociétés de transfert d'argent et géants de l'assurance vont être obligés de s'adapter pour survivre. Elle bouleverse aussi toute l'économie numérique : n'importe quel site commercial que nous utilisons pour acheter un bien ou un service peut être réinventé en version pair à pair. De la vente de musique à la location de logement en passant par le transport à la demande ou les petites annonces, tout est en train d'être reconfiguré par des jeunes sociétés qui veulent concurrencer Apple, Airbnb, Uber ou Amazon, avec des applications blockchain qui mettront en lien producteur et consommateur, sans tiers superflu. La deuxième fonctionnalité, les *smart contracts*, va, elle, servir de tremplin à l'automatisation du monde : toujours plus nombreux, les objets connectés (montres, téléphones, réveils, réfrigérateurs, voitures, etc.) trouvent dans la blockchain la plateforme idoine pour communiquer entre eux. Des processus, pour lesquels l'intervention humaine était nécessaire, vont pouvoir être modélisés, codés et exécutés de manière systématique par des robots et des programmes : le versement d'une prime d'assurance après un accident ou une intempérie, la revente d'énergie par un panneau solaire, la recharge d'une voiture électrique, et même, potentiellement, tout le circuit logistique de production d'un bien, de la découpe d'un arbre en Finlande à sa livraison sous forme de chaise à l'autre bout du monde. Enfin, la dernière fonctionnalité, la notarisation, n'est pas la moins prometteuse : par la possibilité qu'elle offre de sécuriser l'information, de la graver dans un registre qui conservera la vérité des données, elle est l'outil d'une réinvention complète de l'administration publique (qui pourra fonctionner de manière transparente et efficace, comme en Estonie). Mieux encore, elle laisse imaginer une refondation numérique de la démocratie : en sécurisant le vote électronique, la blockchain peut permettre au citoyen de reprendre le pouvoir, d'être directement partie prenante des décisions politiques de son État ou sa collectivité, et d'être mieux entendu, compris et représenté. Une lueur d'espoir à notre époque de crise de la démocratie représentative. Ces révolutions annoncées ne sont pas des promesses sans fondement : chacune d'entre elle est en cours, comme le prouvent les expériences concluantes menées par d'innombrables start-up, des grandes entreprises et des États, et qu'il est temps de découvrir.

CHAPITRE 4

Une révolution financière

Dans la finance, la blockchain est unanimement décrite comme une immense opportunité, car elle permet de réduire drastiquement les coûts de transaction et de fonctionnement dans une industrie devenue trop grosse par rapport à sa valeur ajoutée dans l'économie et qui fournit ses services à un tarif souvent trop élevé. Depuis le milieu du XIXe siècle, l'importance du secteur financier a ainsi considérablement augmenté. Aux États-Unis, selon les calculs de l'économiste français Thomas Philippon, professeur à New York University Stern, l'industrie financière n'y représentait alors que 1,5 % du PIB[1]. Aujourd'hui, son poids est 5 à 6 fois supérieur. En Europe, il a grimpé de 2,3 % à 8,2 % du PIB entre 1951 et 2007, d'après les calculs de l'économiste français Guillaume Bazot, de l'Institut des politiques publiques[2]. Aux États-Unis, d'après les économistes Robin Greenwood et David Scharfstein, de la Harvard Business School, la part de la finance dans le PIB des États-Unis a presque doublé entre 1980 et 2006, passant de 4,9 % à 8,3 %[3]. Cette croissance est en partie justifiée. Le poids des banques a crû au gré des trois grandes révolutions industrielles qu'elles ont accompagnées. « La première grande augmentation, entre 1880 et 1900, correspond au financement des chemins de fer et des premières industries lourdes. La deuxième, entre 1918 et 1933, […] au financement de la révolution de l'électricité, de l'automobile et des entreprises pharmaceutiques. […] La troisième hausse, de 1980 à 2001, […] au financement de la révolution numérique[4] », écrit Thomas Philippon. Mais en grandissant ainsi, les acteurs du secteur financier sont devenus moins compétitifs. Au fil des années 2000 et 2010, ils ont facturé des services trop chers, inutiles ou au risque mal contrôlé[*1]. « Selon un rapport du cabinet McKinsey, les banques retirent un montant stupéfiant de 1 700 milliards de dollars par an, 40 % de leur chiffre d'affaires, des services de paiements internationaux. Plus surprenant encore, malgré toute l'innovation technologique, le coût de l'intermédiation aux États-Unis n'a pas changé de manière significative depuis le début du XXe siècle […]. Alors même qu'un certain nombre de start-up, utilisant Bitcoin pour la plupart, rendent les services

de paiement aussi simples et peu coûteux que l'envoi d'un e-mail[5] », soulignent les experts du FMI Andreas Adriano et Hunter Monroe, dans un article publié en juin 2016.

Cela offre aujourd'hui une opportunité à de nouveaux entrants mieux-disants, qui peuvent, grâce à la blockchain, attaquer les anciens poids lourds avec des services moins onéreux, comme le considère l'investisseur suisse Nicolas Steiner. Basé à Londres, cet expert des « fintechs » (les start-up financières) parie que l'arrivée de la blockchain va faire des ravages. « Les business models de la finance sont tellement surévalués qu'il y a de quoi attaquer. Les banques vont souffrir, car elles sont surpayées pour le service qu'elles produisent, comme les télécoms jusqu'aux années 1990, quand la voix sur IP[*2] les a obligés à se remettre en cause. Elles ne vont pas disparaître, mais c'est la fin des vaches grasses. Elles vont devoir optimiser leur infrastructure. Ce n'est pas facile, car elles sont si vieilles, elles ont tellement de coûts, qu'elles ne savent plus comment y toucher », juge-t-il. Avec la blockchain, les institutions financières ont la possibilité de faire des économies massives de fonctionnement, qui bénéficieront finalement, au moins partiellement, à leurs clients. « La blockchain peut fournir une sécurité des transactions sans précédent à travers la cryptographie, tout en évitant d'utiliser d'onéreux ordinateurs centraux et des centres de serveurs. Cela change complètement le modèle de coût des transactions financières[6] », affirmait un rapport du cabinet de conseil Capgemini en mai 2015. Selon une étude de la banque Santander InnoVentures, cette technologie pourrait réduire les coûts d'infrastructure liés aux paiements internationaux, au trading de titres et à la mise en conformité des banques de 15 à 20 milliards de dollars par an, dès 2022[7], pour l'ensemble du secteur. Selon un autre rapport, publié en octobre 2016 par le cabinet Capgemini, dans l'univers de la banque de détail, « l'industrie des crédits immobiliers bénéficiera grandement de l'adoption des *smart contracts*. Les consommateurs pourraient s'attendre à économiser entre 480 et 960 dollars par crédit et les banques pourront réduire leurs coûts de l'ordre de 3 à 11 milliards de dollars par an […] sur les marchés américain et européen[8] ». Dans la partie banque d'investissement, Capgemini estime qu'en réduisant la durée de transaction et de règlement des prêts syndiqués[*3] aux entreprises, la blockchain permettra « une croissance de 5 à 6 % de la demande à l'avenir, qui apportera entre 2 et 7 milliards de dollars de chiffre d'affaires supplémentaire ».

Dans ces conditions, aucun acteur financier ne pourra se permettre d'ignorer cette révolution, sous peine d'être dépassé par ses concurrents ou par de nouveaux entrants. « D'ici quelques années, un grand nombre de start-up blockchain auront investi le champ des services financiers et différentes plateformes blockchain fournissent déjà des solutions compétitives. Comme pour toutes les technologies émergentes d'importance, plus tôt vous commencez à planifier sa mise en place, mieux ce sera », conseillaient les consultants de Capgemini à leurs lecteurs issus du monde financier. Ce sentiment fait désormais consensus dans le secteur. Selon l'étude menée par l'EFMA et Deloitte, 58 % des institutions financières pensent qu'une partie de leur métier et de la chaîne de valeur sera modifiée, 53 % estiment que l'utilisation de la blockchain sera généralisée d'ici 2 à 5 ans, 20 % d'ici 18 mois à deux ans et 11 % d'ici 12 à 18 mois[9]. Au total 84 % d'entre elles pensent donc qu'elle sera généralisée sous 5 ans. Plusieurs utilisations (« cas d'usage » dans le jargon) sont mises en avant : 60 % des institutions interrogées pensent que la première sera les transferts internationaux de monnaie, 23 % les « systèmes de

compensation et règlement » (des opérations entre banques où elles se versent le solde correspondant à ce qu'elles se doivent), 20 % la lutte antiblanchiment et le KYC (*Know Your Customer*, c'est-à-dire les justifications administratives que le client doit fournir), 19 % le paiement par monnaie fiduciaire et les règlements, et enfin 19 % l'amélioration de la transparence. Sans oublier l'assurance, hors du champ de cette étude, mais qui promet d'être un des secteurs les plus rapidement touchés par la technologie blockchain.

Paiement et transfert d'argent : la révolution est en cours

À ce jour, les seules applications financières de la blockchain qui sont vraiment commercialisées et fonctionnent sont celles qui concernent le paiement et le transfert d'argent à l'international. Elles utilisent pour la grande majorité la blockchain Bitcoin, la plus ancienne et sécurisée.

Des paiements sécurisés

Régler un achat en Bitcoin présente deux avantages majeurs : la sécurité lors du paiement, supérieure à celle des cartes bancaires, et le faible coût de la transaction (particulièrement intéressant sur les petits montants et à l'étranger). Commençons par le premier avantage : avec sa réputation sulfureuse, le Bitcoin peut faire peur aux néophytes. Pourtant, cette cryptomonnaie est peut-être actuellement le moyen le plus sûr de payer en ligne. « Le Bitcoin élimine le risque de fraude à la carte bancaire[10] », explique Marc Andreessen dans un article du *New York Times*. « Avec votre numéro de carte bancaire, on peut faire autant de dépenses que l'on veut », rappelle Manuel Valente, de La Maison du Bitcoin. Tandis qu'avec une adresse publique de Bitcoin, on ne peut rien acheter. D'innombrables entreprises se sont ainsi fait pirater les numéros de cartes bancaires de leurs clients (ainsi que le code à trois chiffres et la date de validité). Fin 2015, les hôtels Hyatt, Mariott et Intercontinental ont annoncé s'être fait dérober plusieurs dizaines de milliers de numéros. En 2013, le géant américain de la grande distribution, Target, avait fait mieux encore : 40 millions de numéros de cartes bancaires subtilisés ! Or, « quand vous payez avec des Bitcoins sur un site, vous n'êtes pas dépendant d'un serveur central », insiste Pierre Noizat, de Paymium. Il suffit d'ouvrir une application dédiée sur votre mobile (par exemple celle de Paymium ou celle de la Maison du Bitcoin), de taper l'adresse du paiement du commerçant (la clé publique) ou de la scanner sous forme de QR code, et de valider la transaction. Le site (ou le commerçant) à qui vous faites ce paiement ne récupère aucune coordonnée bancaire, seule votre clé publique apparaît dans la blockchain : il n'y a rien à pirater. Si d'aventure votre propre ordinateur était piraté et qu'un logiciel espion récupérait vos logins, mots de passe ou clés privées, il existe des solutions techniques pour se prémunir d'un vol. La société Ledger, maison mère de La Maison du Bitcoin, propose un portefeuille de

cryptomonnaie qui apporte cette sécurité supplémentaire : une clé USB appelée « Ledger Wallet ». Ce gadget (qui coûte 69 euros), doté d'un petit écran et de deux boutons, permet de stocker les clés privées et de réaliser des paiements sans que celles-ci ne soient communiquées à l'ordinateur sur lequel a lieu la transaction. Ainsi, même si l'ordinateur est espionné par un logiciel, la clé privée ne sort pas du « Ledger Wallet ». Elle ne peut donc pas être volée. « Je ne cours donc aucun risque si l'ordinateur est vérolé. Si l'application elle-même était vérolée, l'écran sur la clé me permet de vérifier que j'envoie bien l'argent vers la bonne adresse », précise Manuel Valente.

Un coût de transaction minime

Le deuxième grand avantage du Bitcoin est le coût des transactions, qui est quasi nul. « Dans le système de l'argent conventionnel, il y a beaucoup d'intermédiaires, qui prélèvent des frais de carte bleue et de tenue de compte », note Joan Noguera, représentant en France de la start-up catalane BTC facil, qui commercialise des distributeurs de Bitcoins. « Avec le Bitcoin, poursuit-il, tout cela s'efface. Il n'y a pas de frais pour payer, seulement des frais pour acheter ou revendre des Bitcoins. » En 2016, détenir une carte bancaire Visa Classic (la plus répandue) coûtait en moyenne en France 40,28 euros par an[11], selon le site Cbanque. Payer pour avoir le droit de payer, avec le Bitcoin, c'est fini. Chez Paymium par exemple, transférer de l'argent d'un compte Bitcoin à un autre ou régler un e-commerçant en Bitcoin se fait sans frais. Attention : utiliser des Bitcoins a tout de même un coût. Les intermédiaires qui vous permettent de vous procurer des Bitcoins se rémunèrent sur l'achat ou la revente de cette cryptomonnaie (comme des comptoirs de change). Il existe toute sorte de façons de se procurer des Bitcoins, mais selon la solution que vous retenez, la commission de l'intermédiaire varie très fortement. Vous pouvez les acquérir en ligne directement sur une grande plateforme de change, comme Kraken, qui prélève 0,26 % de votre achat de Bitcoins. Vous pouvez passer par une « banque Bitcoin », comme Paymium, qui vous facilite le processus d'acquisition, mais prend une commission plus importante (0,59 %). Vous pouvez aussi vous rendre à un distributeur automatique de Bitcoins (un « ATM »), comme ceux installés à Montpellier par la société BTC facil (qui prélève 6 % de frais à l'achat, 4 % à la revente), ou en Suisse par les start-up Bitcoin Suisse ou SweePay (qui donne la possibilité, depuis fin octobre 2016, d'acheter des Bitcoins directement dans les automates de billets de train des gares suisses, en association avec la compagnie de chemin de fer nationale CFF). L'utilisation de ces « ATM Bitcoin » est très simple : « Vous donnez le numéro de votre wallet ou montrez votre QR code, vous insérez un billet en euros, et en une seconde, vous avez acquis vos Bitcoins[12] », précise Joan Noguera. Le distributeur permet également de retirer, aussi facilement, des euros à partir du compte Bitcoin. Toutefois, ces ATM sont encore rares, et jouent surtout un rôle de communication pour démocratiser le Bitcoin. Enfin, vous pouvez obtenir des Bitcoins très facilement avec du liquide à un comptoir de change (comme La Maison du Bitcoin, à Paris, qui prend environ 10 % de commission). « Comme les plateformes de change sur Internet sont un peu complexes à utiliser, nous avons ouvert ce comptoir où changer en espèces ou en carte bleue. Ça prend

trois minutes : vous donnez un billet et une pièce d'identité valide (carte d'identité, passeport ou permis de séjour), et voilà », explique Manuel Valente, de La Maison du Bitcoin.

Quand est-il avantageux de payer en Bitcoins ?

Si l'on prend en compte les commissions prélevées pour acquérir des Bitcoins, l'avantage de coût du Bitcoin dépend des usages. Pour les achats de tous les jours, cela reste plus simple et moins coûteux pour le client de payer en euros, que ce soit en liquide ou par carte. Mais les commerçants, eux, ont à y gagner. Lors des paiements par carte bancaire, ils doivent s'acquitter d'une commission auprès de leur banque dont une partie est fixe, c'est pourquoi beaucoup refusent la carte bancaire sur les petites transactions (moins de 10 euros), qui ne sont pas rentables pour eux. Quand ils acceptent le Bitcoin, ils ne paient aucune commission, mais un abonnement vite rentabilisé (19,90 euros par mois chez Paymium). « Quand on a besoin d'échanger des sommes faibles, les frais de transaction sont en général déraisonnables par rapport au montant. Passer par une blockchain [comme Bitcoin] permet d'abaisser singulièrement le coût de transaction, donc de rendre intéressant ces micropaiements[13] », confirme Éric Lévy-Bencheton, expert blockchain au cabinet de conseil Keyrus. Enfin, l'avantage de coût du Bitcoin est particulièrement fort pour les transactions effectuées à l'étranger (et les transferts d'argent à l'international, comme nous le verrons juste après). Selon une étude comparative du site Cbanque, en moyenne, fin 2015, un paiement de 100 euros par carte à l'étranger coûtait 2,77 euros. Le Bitcoin, lui, ne connaît pas les frontières. Aucun frais supplémentaire ne s'applique donc si la transaction a lieu à l'étranger. Si vous avez acheté vos Bitcoins en ligne à une plateforme de change ou à une banque Bitcoin, les commissions d'achat et de revente sont très inférieures aux commissions bancaires d'un paiement à l'étranger : mieux vaut donc payer en Bitcoins qu'en carte bancaire.

Il y a néanmoins un dernier aspect à prendre en compte : l'évolution du taux de change du Bitcoin par rapport à la monnaie utilisée pour l'acquérir. Si vous choisissez de payer en Bitcoin alors que le prix du bien acquis est en euros (ou dans une autre monnaie traditionnelle), vous allez sans doute dépenser vos Bitcoins à une cotation différente de celle à laquelle vous les avez achetés : c'est ce que l'on appelle un risque de change. Il est possible de faire une mauvaise affaire si le cours du Bitcoin a plongé ou une excellente s'il s'est envolé. Vous pouvez limiter ce risque en changeant vos Bitcoins dans la journée de l'achat. Si l'on se place du point de vue des commerçants, des systèmes leur permettent d'être réglés en Bitcoins et de voir l'argent échangé instantanément dans la monnaie courante, sans même qu'ils n'aient à s'en préoccuper, afin de geler le risque de change.

Payer en Bitcoins, mode d'emploi

Mais comment exactement procéder pour faire un paiement en Bitcoins ? Bonne nouvelle : ce n'est pas très compliqué. Pour ma part, j'ai essayé chez Paymium, qui présente l'avantage d'être associé, pour

la gestion de ses comptes, à la société Aqoba, agréée par l'Autorité de contrôle prudentiel et de résolution (ACPR). La procédure d'ouverture de compte est un peu lente, mais très simple. J'ai commencé par créer un compte sur le site de Paymium (en créant un login et un mot de passe), puis j'ai reçu un e-mail de confirmation, et accepté les conditions d'utilisation. Celles-ci précisent en particulier le principal danger que j'encours : me faire dérober mon identifiant et mon mot de passe. « Les clients ne doivent communiquer leurs mots de passe à aucune tierce personne et sont tenus de préserver leur confidentialité en toutes circonstances. Ils sont également tenus, lorsqu'ils utilisent Internet ou Internet mobile, de prendre les mesures nécessaires pour préserver un niveau de sécurité élevé sur leur matériel informatique », indique la note. Il faut ensuite remplir un formulaire classique (nom, nationalité, pays de résidence, adresse, date de naissance, ville de naissance). J'obtiens un numéro de compte. J'ai alors créé un compte à deux tiroirs : l'un en euro, l'autre en Bitcoin. Il faut d'abord alimenter le tiroir en euros, avant de faire le change en Bitcoin. Je fais un virement de 100 euros depuis mon compte bancaire habituel vers le compte de Paymium (qui est domicilié en Belgique, sans doute était-ce plus facile que de le créer en France), en indiquant mon numéro de compte Paymium. Quelques jours plus tard, quand le virement bancaire a été effectué, je convertis chez Paymium mes euros en Bitcoins au cours de 1 Bitcoin pour 516,03 euros (commission de change de 0,59 % incluse). Je reçois instantanément 0,1938 Bitcoin. Ça y est, je possède un compte en Bitcoins.

Mais que faire avec ? Payer ! Pour cela, je télécharge l'application Hot Wallet de Paymium, qui est l'équivalent d'un porte-monnaie sur le mobile. Je tape mon login et mon mot de passe. On me demande de créer un mot de passe supplémentaire et on me fournit une phrase de *back up* (récupération du compte) qui correspond à une succession aléatoire de 12 mots. Je la note quelque part chez moi – et la cache ! Elle me permettra de récupérer mon « wallet » si quelqu'un dérobe ou casse mon téléphone. Il faut ensuite transférer de l'argent de mon compte Paymium vers ce wallet (comme on sortirait des billets d'un coffre pour les mettre dans un portefeuille). J'envoie 0,019 Bitcoin, soit l'équivalent de 10 euros à ce moment-là, simplement en me rendant sur mon compte en ligne Paymium et en indiquant l'adresse publique de mon wallet (qui est changée régulièrement pour des raisons de sécurité). Je reçois un e-mail avec un lien sur lequel cliquer pour confirmer l'opération. Je récupère deux à trois heures plus tard la somme dans mon wallet. Avec ce wallet, je peux payer très facilement sur plus de 100 000 sites Web[14], dont Showroomprivé, Expedia, Wikipedia, Wordpress ou Microsoft. Je peux aussi le faire chez les commerçants, plus rares, qui acceptent ce type de paiement. Ils sont recensés et géolocalisés sur le site CoinMap.org. À Paris, à l'automne 2016, le site en dénombrait 31 (dont des pizzerias, des appartements à louer, des boutiques de vêtements et des bars, comme le Sof's Bar, rue Saint-Sauveur, où se retrouve la communauté Bitcoin parisienne, ou la brasserie O'Caire, rue du Caire dans le II^{e} arrondissement). L'achat est très simple. Personnellement, j'ai commandé sur Showroomprivé un pull rayé gris et noir pour ma compagne, en solde, pour un total de 14,99 euros (une affaire), frais de livraison inclus (soit 0,019417 Bitcoin). Au moment de régler, il suffit de sélectionner Bitcoin plutôt que Visa, Mastercard ou Paypal. Une page s'affiche avec le montant en Bitcoin, une adresse et un QR code (la traduction de cette adresse en un code à scanner). Avec l'appli Hot Wallet, je scanne le QR code et envoie les fonds. Moins d'une

minute après, c'est réglé, et je n'ai laissé aucune coordonnée bancaire nulle part. Quelques jours plus tard, j'ai réitéré l'opération dans un café, le O'Caire. Il m'a fallu seulement quelques secondes pour scanner le QR code de l'établissement sur l'Ipad du barman, et envoyer le 0,00142 Bitcoin correspondant à 1,20 euro pour un expresso serré au comptoir. Payer en Bitcoins est donc à la portée de tout le monde, à condition de posséder un smartphone.

Il est difficile de connaître le nombre d'utilisateurs de Bitcoins en France. À l'été 2016, Paymium, qui fait partie des sociétés leaders du secteur, comptait environ 100 000 clients, aux deux tiers français, dont 15 000 à 20 000 véritablement actifs. À long terme, certains imaginent une utilisation plus révolutionnaire encore du réseau Bitcoin pour le paiement, en se fondant sur la technique des *colored coins* (jetons colorés). C'est le cas de la start-up Czam, cofondée par Adrian Sauzade : « L'idée est de prendre quelques centimes de Bitcoins, de les transférer sur le réseau Bitcoin et de leur donner une autre valeur[15] », résume-t-il. Ces centimes ou millièmes de Bitcoins ne sont alors plus utilisés pour leur valeur propre, mais seulement comme des jetons qui représentent par exemple un point de fidélité, un ticket ou même une action. Ces actifs, représentés sur la blockchain par ces *colored coins*, deviennent ainsi transférables numériquement, en toute sécurité. « Notre vision, c'est que dans dix ans, tu pourras payer ton café avec une action de Facebook, ou une part de Tesla, à la valeur du jour, qui sera comme de la monnaie », explique Adrian Sauzade. « L'idée, c'est de rendre les marchés liquides », poursuit-il : tout pourrait devenir une monnaie d'échange inscrite dans la blockchain Bitcoin.

Transférer de l'argent d'un pays à un autre

Actuellement, envoyer de l'argent à l'étranger (hors Europe) ou en recevoir coûte cher, que vous passiez par votre banque ou par une société spécialisée (comme Western Union ou MoneyGram). La Société générale, par exemple, prélève un forfait minimum de 13,75 euros (sans compter les commissions de change et de port) pour émettre un virement international (hors Europe) et de 17,50 euros pour en recevoir (pour une somme supérieure à 150 euros)[*4]. Chez HSBC, la commission atteint 12,50 euros pour l'émission du virement international et 25 euros pour la réception. Si vous passez par une société spécialisée, l'addition est un peu moins lourde, mais tout de même salée : selon un rapport publié en avril 2014 par le *think tank* britannique Overseas Development Institute (ODI), Western Union prélevait en moyenne 9,4 % de l'argent envoyé vers l'Afrique et son rival, MoneyGram, 10,4 %[16].

De nombreuses applications fondées sur la technologie blockchain permettent d'effectuer le même service à un coût bien moindre. Les plus développées sont Align Commerce (qui vise surtout une clientèle de PME) et Abra (pour les particuliers). L'une et l'autre se présentent comme des services Web de transfert d'argent ultracompétitifs, mais ne mettent pas du tout en avant leur usage de la blockchain Bitcoin. Car l'essentiel, pour le consommateur, c'est le prix. « Abra masque la complexité et l'existence du Bitcoin au consommateur, il n'a pas besoin de s'en préoccuper, la somme qu'il envoie est complètement protégée, qu'elle soit en euros, en dollars ou dans toute autre monnaie traditionnelle[17] », précise Bill Barhydt, le PDG d'Abra. Avec cette application, la commission atteint environ 2 % en

moyenne. « Notre idée était de créer un système de paiement mondial qui permette aux gens de s'envoyer de la vraie monnaie (dollar, euro, etc.) facilement, entre deux numéros de téléphone à deux coins du globe. Vous êtes à Paris, vous avez de la famille au Vietnam ? Vous pouvez utiliser une simple application pour transférer l'argent », résume le fondateur. « Quand vous faites cela, il n'y a pas de banques au milieu de la transaction, ni au départ, ni à l'arrivée. Le système est pair à pair. Abra élimine les intermédiaires et fait chuter le coût du transfert », affirme-t-il. Le fonctionnement est très simple : pour envoyer de l'argent, il suffit de déposer la somme voulue sur son compte Abra en faisant un virement bancaire ou en apportant la somme en liquide à un membre du réseau Abra, géolocalisé autour de vous par l'application (comme un chauffeur Uber). Ces agents de change, constitués d'utilisateurs volontaires de l'application, sont appelés *tellers*. Une fois l'argent sur le compte, il suffit de le transférer à la personne de son choix (qui doit avoir préalablement téléchargé l'application et s'être créé un compte sur celle-ci). La somme est instantanément reçue. Le destinataire peut alors soit l'envoyer sur son compte bancaire (en monnaie locale), soit repérer un *teller* autour de lui pour obtenir le montant en liquide, contre une commission (2 % en moyenne). L'application Abra se rémunère sur la commission prélevée par ce membre du réseau (exactement comme Uber avec ses chauffeurs). Testé pour l'instant uniquement entre les États-Unis et les Philippines, l'application, qui sera lancée dans les mois à venir en Europe, rencontre déjà un grand succès. « Nous avons d'excellents retours des consommateurs, qui sont surpris par la simplicité d'utilisation », se réjouit Bill Barhydt. Le potentiel de cette jeune start-up californienne basée à Mountain View, dans la Silicon Valley, n'a pas échappé au géant American Express, qui a investi dans l'entreprise en octobre 2015, lors d'une levée de fonds de plus de 14 millions de dollars.

Un marché gigantesque qui suscite la convoitise

Si Abra a suscité une telle convoitise chez les investisseurs, c'est que le marché potentiel pour ce type de service est immense. En 2016, le montant total envoyé vers les pays à faibles et moyens revenus devrait atteindre 442 milliards de dollars, selon les estimations de la Banque mondiale (dont environ 65 milliards vers la Chine, autant vers l'Inde et plus de 29 milliards vers les Philippines)[18]. Pour les centaines de millions de travailleurs immigrés qui envoient de l'argent vers leur pays d'origine et pour leurs familles qui en reçoivent, le Bitcoin est une véritable chance, comme le souligne l'investisseur Marc Andreessen : « En passant par le Bitcoin avec pas ou peu de frais, ces transferts transfrontaliers vont permettre d'augmenter la qualité de vie des travailleurs immigrés et de leurs familles de manière significative. En réalité, il est difficile d'imaginer quoi que ce soit qui ait un effet plus rapide et plus positif sur tant de gens dans les pays les plus pauvres du monde[19] », écrivait-il dans le *New York Times*. Les premiers ciblés par ces services l'ont bien compris et n'ont pas attendu le développement de ces applications spécialisées pour utiliser le Bitcoin. À la Maison du Bitcoin, à Paris, une bonne partie de la clientèle du comptoir de change est ainsi constituée de travailleurs étrangers qui envoient de l'argent à leur famille. Chez nos voisins helvètes, selon Niklas Nikolajsen, le fondateur de Bitcoin Suisse,

« environ la moitié des clients de nos distributeurs automatiques de Bitcoin installés en Suisse les utilisent pour transférer de l'argent dans leur pays d'origine[20] ».

Les services blockchain de transfert d'argent ont un autre effet positif : ils permettent d'inclure dans le système financier les quelque 2 milliards d'adultes qui en sont exclus, selon la Banque mondiale[21]. Avec le système de *tellers* d'Abra par exemple, il n'est plus nécessaire de détenir un compte bancaire pour envoyer et recevoir de l'argent : un smartphone suffit. *Idem* pour Monetas, une autre start-up, basée à Zoug en Suisse, qui utilise aussi une cryptomonnaie pour faire chuter les coûts de transaction sur sa plateforme de paiement par mobile. « Nous nous focalisons sur les marchés en développement : 80 % des Africains ne sont pas bancarisés, ils seront les premiers bénéficiaires de nos services[22] », explique Vitus Amman, directeur marketing de Monetas. La start-up a effectué un premier test en Tunisie et veut lancer une application pilote en juin prochain.

Les banques, condamnées à changer pour survivre

Dans le monde financier, les acteurs du paiement et du transfert d'argent à l'international sont les premiers touchés par la blockchain. Mais toutes les autres activités bancaires sont potentiellement concernées à moyen terme. Les grands acteurs du secteur s'y préparent, tout en restant sereins, convaincus que la blockchain est plutôt pour eux une solution pour réduire leurs coûts de fonctionnement et augmenter leur marge qu'une véritable menace existentielle. « Notre industrie est très fortement candidate à être transformée par la blockchain[23] », confirmait Nicolas Rivard, responsable de l'innovation chez Euronext Paris (l'opérateur financier de la bourse de Paris, Amsterdam et Bruxelles), lors du Forum parlementaire de la blockchain, le 3 octobre dernier dans la capitale française. « À court terme, nous ne sommes pas sur des projets de transformation de la chaîne de valeur, plutôt sur des projets d'amélioration de l'efficacité, avec des gains possibles de 30 à 50 % », estimait-il. Gare aux retardataires : « Les acteurs qui ne s'y mettent pas vont disparaître », avertissait l'expert. Mais ceux qui auront l'intelligence de s'adapter sortiront sans doute plus solides encore de cette transformation. « Les banques ont besoin de repenser leur modèle de valeur[24] », admet Emmanuel Méthivier, le président du CA Store (Crédit agricole). Comme d'autres, il n'est pas vraiment inquiet pour l'avenir des banques. « Elles pourront survivre en trouvant des pépites autour de la blockchain, car il restera toujours de vrais besoins de tiers de confiance [notamment pour la vérification d'identité]. Sur le Bitcoin par exemple, vous n'êtes pas vous, mais un numéro, une clé privée. Si je veux faire un virement, quelqu'un peut m'envoyer une fausse clé publique », relève-t-il. L'économie continuera donc à avoir besoin des banquiers.

De premières expérimentations

Avec curiosité mais sans crainte, toutes les banques ou presque mènent donc, chacune de leur côté, des recherches sur les applications de la blockchain. Le département d'innovation du Crédit agricole, le CA Store, a ainsi tenté une expérience pionnière pendant plusieurs mois. « Nous nous sommes intéressés à la notarisation, c'est-à-dire à l'enregistrement des informations sur la blockchain », raconte Emmanuel Méthivier. « Nous travaillons avec des développeurs d'applications mobiles, qui sont payés au nombre de connexions par mois sur leur application. Or, jusqu'à présent, nous n'avions jamais les mêmes chiffres de connexion qu'eux. Maintenant, les connexions aux applications sont enregistrées sur la blockchain Bitcoin. Les développeurs sont payés directement en Bitcoins », précise-t-il. L'expérience s'est avérée plutôt concluante : « les transactions ont été enregistrées en moyenne en 10 minutes, alors que nous nous attendions à ce que cela dure plus longtemps. Dix minutes de délai, ce n'est pas gênant, sachant que nous payons habituellement nos développeurs au mois » constate-t-il.

Parallèlement à ces expérimentations solitaires, de nombreux acteurs du secteur financier se sont regroupés dans des consortiums pour mutualiser les coûts de recherche, avancer plus vite et définir des standards et des outils communs. Aux États-Unis, R3 développe sa blockchain privée Corda pour les opérations interbancaires. En France, l'initiative la plus significative est menée par la CDC, qui fédère, depuis début 2015, 25 institutions financières dans Labchain, un laboratoire d'innovation blockchain commun (dont le Crédit agricole, Axa, BNP Paribas, La Banque postale, BPCE…). « En France, l'écosystème est petit, c'était donc intéressant de le fédérer. Cela permet également de mutualiser les coûts de veille. Nous avons rapidement proposé à d'autres acteurs de la place de nous rejoindre et avons lancé Labchain début 2015[25] », raconte Nadia Filali, qui copilote le projet à la CDC. « Tout le monde commençait alors à se rendre compte qu'il n'était pas impossible que ce soit une vraie révolution technologique, mais elle semblait difficile à appréhender, nous avions tous un niveau de connaissance faible, il pouvait être pertinent de faire de la recherche ensemble[26] », se souvient Laurent Benichou, d'Axa France. D'un espace d'échange et de partage sur la blockchain, Labchain s'est peu à peu transformé en laboratoire de projets concrets. « Nous regardons au travers de nos expérimentations ce qui réduit les coûts de fonctionnement des processus, mais surtout les opportunités de nouvelles offres et services qu'apporte la blockchain », résume Nadia Filali. Les projets les plus avancés sont arrivés au stade du prototype (appelés « poc » dans le milieu, pour *proof of concept*, c'est-à-dire un « système expérimentable »). Trois « pocs » ont à ce jour été lancés par Labchain : le premier sur la simplification des procédures d'identification du client, le deuxième sur des « collatéraux » (des garanties de prêts), et le dernier sur l'assurance décès (pour automatiser le versement et simplifier les démarches des proches).

Des applications bancaires pour les particuliers

Concrètement, quels services bancaires sont véritablement en train d'être transformés par la blockchain ? Commençons par les applications qui concernent le plus directement les particuliers. La blockchain va d'abord permettre d'éliminer, ou presque, l'interminable documentation administrative à remplir à chaque fois que l'on veut ouvrir un compte, une assurance vie ou obtenir un prêt auprès d'une

banque. Dans le jargon du milieu, cet ensemble de procédures pour obtenir des informations du client, obligatoires légalement pour des impératifs de lutte antiblanchiment, s'appelle KYC (*Know Your Customer*). Outre la CDC, qui y travaille au sein de son laboratoire Labchain, beaucoup de start-up et de grands groupes se penchent sur cette question. C'est le cas de la pépite française Stratumn. « Aujourd'hui, ouvrir un compte est un process très lourd. On pourrait imaginer une solution où vous auriez une sorte de carte d'identité stockée dans la blockchain. Quand vous ouvrez une première fois un compte en banque, on vous donne un jeton électronique qui prouve que votre identité a déjà été vérifiée. Vous pourrez ensuite utiliser ce jeton pour ouvrir un autre compte[27] », suggère François Dorléans. Et ce, même dans une enseigne concurrente. « Idéalement, il faudrait qu'il n'y ait plus qu'une seule place de marché du KYC, comme nous le proposons », ajoute-t-il. En résumé, si vous ouvrez un jour un compte à la Banque postale, qui fait les vérifications nécessaires, plus besoin ensuite de reproduire le même ensemble de documents quand vous demandez un PEA chez LCL ou une assurance vie chez BNP Paribas. IBM France s'est aussi lancé dans la même démarche, avec Crédit mutuel Arkéa, et a dévoilé un premier prototype. « La blockchain va être utilisée pour tracer toutes les pièces justificatives qu'un client a soumises à n'importe quelle entité du groupe. Cela permet de simplifier les processus administratifs internes[28] », précise Luca Comparini, d'IBM France. Dans un deuxième temps, le projet pourrait aller plus loin : « On a pour idée d'étendre ce réseau à des partenaires externes, par exemple un réseau de magasins de la grande distribution, un fournisseur d'accès d'Internet ou la Poste », imagine-t-il.

Prêter et investir sur la blockchain

La blockchain trouve aussi de premières applications dans les deux activités traditionnelles des banques, auxquelles elle invite les particuliers à se mêler : le prêt et l'investissement. La start-up américaine Consensys a développé un premier prototype de prêt participatif sur Ethereum : EtherLoan. Son fondateur, Joseph Lubin, résume le concept : « Imaginons que je veuille acheter quelque chose, puis-je obtenir un microprêt de votre part alors que vous êtes à l'autre bout de la planète[29] ? » Consensys travaille également au développement d'une plateforme d'investissement participatif (*crowfunding*) sans intermédiaire sur Ethereum : Weifund. En la matière, une première expérience retentissante a été menée au printemps 2016. Baptisée TheDAO, une « organisation autonome décentralisée » (DAO) a été lancée le 30 avril 2016, à l'initiative de deux start-up, l'Allemande Slock.it et la Suisse Bity SA. Conçue comme un logiciel constitué d'un ensemble de *smart contracts* (des programmes informatiques qui automatisent l'exécution de contrats) entre les investisseurs, inscrits sur la blockchain Ethereum, TheDAO se voulait un fonds d'investissement sans management, régi par du code *open source*, et censé miser sur des projets choisis par les actionnaires. L'initiative a été accueillie avec un peu trop d'enthousiasme : 11 000 actionnaires se sont précipités sur la levée de fonds réalisée en mai, apportant, en Ethers, l'équivalent de quelque 168 millions de dollars. Las, courant juin, des hackers non identifiés réussissaient à détourner plus de 50 millions de dollars en inscrivant un code vérolé dans la blockchain Ethereum. La mésaventure a fait couler beaucoup d'encre, non seulement car ce piratage a remis en cause

la sécurité de la blockchain Ethereum, mais aussi car la solution apportée pour protéger les victimes de la fraude a fait débat : une majorité d'utilisateurs d'Ethereum a voté pour revenir en arrière, annuler toutes les transactions qui ont suivi le hack et réécrire l'histoire des opérations à partir du dernier bloc qui précédait l'inscription du code malveillant. Avec une telle manœuvre, appelée « fork », la blockchain Ethereum perdait son caractère d'irréversibilité, un attribut pourtant fondamental des blockchains.

Stephan Tual, un des cofondateurs de Slock.it qui fut à l'origine de cette expérience malheureuse, regrette d'être allé trop vite, sans avoir prévu de garde-fous : « Comme le code, une fois inscrit, est immuable, il aurait fallu du code 100 % sans erreur, mais malheureusement ça n'existe peut-être pas. On peut s'en rapprocher (les fusées Ariane ou la Nasa ont des taux d'erreur très faibles), mais on ne peut pas l'atteindre. Ce qui aurait sauvé la DAO, c'est de prévoir un système qui permette de dire stop s'il y a un problème, de changer le code et de redémarrer. C'est comme les bicyclettes pour enfants. Sur des tels projets décentralisés, il faut d'abord mettre des petites roues, puis progressivement les enlever. On ne l'a pas fait car on ne s'attendait pas du tout à un tel succès[30]. » À terme, Stephan Tual n'abandonne pas l'idée de retenter l'expérience, avec plus de prudence : « On s'y remettra vers le milieu de l'année 2017, pas avant. On va se pencher en particulier sur des cas "non profit" [à but non lucratif]. Dans les organisations caritatives, la DAO permettrait de s'assurer que les fonds sont bien versés là où on veut. C'est l'avantage des DAO : chacun peut voter sur l'allocation des fonds, à la hauteur de ce qu'il investit. C'est la démocratie directe. »

En France, le financement participatif sur la blockchain se développe également, mais de manière bien plus encadrée et sécurisée. Fin mars 2016, lors des troisièmes assises du financement participatif, le ministre de l'Économie de l'époque, Emmanuel Macron, a autorisé l'expérimentation pionnière de minibons : des sortes d'obligations émises par des PME pour se financer et pouvant être échangées sur une blockchain. L'objectif est de développer le financement participatif des PME auprès d'autres entreprises ou de particuliers. Six mois plus tard, mi-septembre, la banque BNP Paribas a annoncé le développement d'une première blockchain dédiée aux minibons, en partenariat avec les start-up françaises Enerfip, Lendosphere et Lumo.

Plus d'efficacité dans les relations entre banques ou entre banques et entreprises

Hors du KYC, du prêt et de l'investissement participatif, il existe de très nombreuses autres applications de la blockchain dans la finance, mais qui concernent plutôt les relations de banques à entreprises, de banques à banques et les processus internes à celles-ci. L'investisseur suisse Nicolas Steiner, cofondateur de l'accélérateur de start-up financières Level39 à Londres, dénombre au moins six domaines (sans compter le paiement) dans lesquels la blockchain va permettre aux acteurs financiers de baisser les coûts et d'améliorer l'efficacité. « D'abord, la simplification des opérations : la blockchain élimine les efforts pour faire des réconciliations (c'est-à-dire s'assurer que les mêmes montants sont bien inscrits dans la comptabilité de l'entreprise et sur le compte à la banque). Ensuite, l'amélioration de la

régulation : elle donne la possibilité aux autorités de contrôle de surveiller en temps réel les opérations qui y sont enregistrées. Il y a également un intérêt en matière de réduction des risques de contrepartie : avec la blockchain, la transaction est sécurisée, plus besoin d'avoir confiance en l'autre. Puis en matière de *clearing settlement* : plus besoin d'intermédiaires qui vérifient la validation des transactions (Swift par exemple est en grand danger). Cinquième aspect : la gestion du capital et des liquidités, à laquelle la blockchain va donner beaucoup plus de transparence (c'était un des gros problèmes de la crise de 2008, ça ne s'est pas beaucoup amélioré jusqu'ici). Enfin, la minimisation des fraudes, car la blockchain permet de regarder tout l'historique des opérations, leur provenance et leur destination[31]. »

Des projets concrets sont déjà lancés, par exemple sur le créneau du règlement d'opérations internationales entre banques ou entre entreprises, sur lequel s'est positionnée la start-up Ripple (qui a lancé la troisième plus grande blockchain en termes de capitalisation actuellement). Selon un rapport de l'agence de notation Moody's, « Ripple a créé un protocole de paiement et un réseau d'échange doté d'un système de consensus bien plus rapide que celui du Bitcoin et a introduit sa propre cryptomonnaie, XRP. […] Beaucoup de grandes banques mondiales sont devenues partenaires de Ripple pour améliorer leurs services de paiement internationaux [plus de 15 à ce jour, dont Santander, UniCredit, Bank of America et UBS][32] ». Le service a déjà été utilisé avec succès. Sept grandes banques ont effectué en juin 2016 de premiers paiements transfrontaliers avec de la monnaie numérique XRP, qui a permis un règlement quasi instantané pour des opérations qui mettaient autrefois plusieurs jours à être finalisées[33].

Dans le domaine des marchés de capitaux, l'opérateur de la bourse technologique de New York, le Nasdaq, a lui aussi commencé à utiliser la blockchain pour la cession de titres non cotés. La première opération a été réalisée en décembre 2015, explique le rapport de Moody's : « Nasdaq a développé, en collaboration avec la start-up Chain, une blockchain, Nasdaq Linq, pour échanger des actions d'entreprises non cotées. En décembre 2015, un émetteur, en l'occurrence Chain, a effectué une première transaction réussie de titre auprès d'un investisseur sur la blockchain Nasdaq Linq. Le titre de propriété a été numérisé, le temps de règlement de l'opération a été significativement réduit et le besoin de certificat papier pour les actions a été éliminé[34]. » Une réussite dont s'est félicitée l'entreprise : « La blockchain a le potentiel de réduire de 99 % le temps de règlement de la transaction et l'exposition au risque dans les marchés de capitaux[35] », commentait le communiqué de presse de Nasdaq annonçant l'opération.

Dans une activité comparable, le trading (l'échange de titres cotés), la blockchain est utilisée par la banque Barclays pour accélérer et automatiser les formalités administratives, en réduire le coût et le risque d'erreur ou de fraude. L'institution britannique a ainsi collaboré avec la start-up Wave, qui a développé un système pour dématérialiser toute la documentation qui accompagne les opérations financières. Début septembre 2016, Barclays et la start-up Wave ont enregistré la première opération financière internationale de trading de l'histoire sur une blockchain. Toute la documentation accompagnant la transaction, entre les sociétés Ornua et Seychelles Trading Company, a été gérée sur la plateforme de Wave. « À l'heure actuelle, les transactions de ce type impliquent souvent un grand nombre de participants dans différentes juridictions partout dans le monde, ce qui se traduit par beaucoup de documents à remplir, signer et envoyer. Le nouveau système de Wave, fondé sur la blockchain, utilise la

technologie des registres décentralisés pour garantir que toutes les parties au contrat peuvent voir, transférer les titres et transmettre les documents à travers un réseau décentralisé sécurisé, rendant plus efficace le commerce international. Ce nouveau système pourrait accélérer les transactions, réduire les coûts pour les entreprises partout dans le monde et réduire le risque de fraude administrative[36] », précisait un communiqué de la banque Barclays.

Enfin, la compagnie Nasdaq a mené une expérimentation fructueuse pour mieux consulter les actionnaires : début février 2016, elle a annoncé avoir développé un système de vote électronique sécurisé sur la blockchain pour les porteurs d'actions d'entreprises cotées à la bourse de Tallinn, en Estonie. L'authentification des votants est assurée par le système de carte d'identité numérique qui existe dans ce pays balte à l'extrémité du nord-est de l'Europe. La blockchain, par son caractère décentralisé, permet en effet de garantir la fiabilité d'un vote électronique : dans un scrutin électronique classique, tous les votes sont rassemblés sur un serveur central, où ils sont à la merci de celui qui détient le serveur ou d'un hacker. Avec la blockchain, ils sont inscrits dans le réseau, enregistrés dans chaque nœud de celui-ci, et ne peuvent pas être altérés (de même qu'une transaction validée dans la blockchain ne peut plus être effacée). Pour la compagnie Nasdaq, proposer un vote électronique sûr aux actionnaires va permettre des échanges bien plus nombreux et fluides entre ceux qui possèdent l'entreprise et ceux qui la dirigent. « En rendant le vote électronique plus efficace et plus sûr, ce système basé sur la blockchain peut donner plus de pouvoir aux actionnaires et mieux les impliquer[37] », commentait un communiqué de la compagnie.

Les banques centrales contre-attaquent

À l'origine, les cryptomonnaies comme le Bitcoin ont été conçues comme des monnaies numériques sans banques centrales, émises par la validation des transactions sur le réseau. Aussi paradoxal que cela puisse-t-il paraître, certaines banques centrales (comme celles d'Angleterre, de Suède, du Canada, de Chine ou de Singapour) s'intéressent pourtant de très près à celles-ci et à leurs systèmes de blockchain (qu'elles appellent aussi « registres distribués »), tentant de l'adapter de manière à conserver leur rôle. « Les aspects monétaires des devises électroniques privées [comme le Bitcoin ou l'Ether] ne sont pas souhaitables du point de vue des gouvernants, mais l'innovation représentée par de tels systèmes de paiement est intéressante. Il est important de souligner que ces deux aspects des devises électroniques privées sont distincts : il serait tout à fait possible techniquement de mettre en place un système de paiement distribué dans le style du Bitcoin, qui utiliserait toutefois une monnaie traditionnelle[38] », affirment John Barrdear et Michael Kumhof, deux économistes de la banque d'Angleterre, dans un article de recherche publié en juillet 2016. Ils ont ainsi imaginé un système de monnaie électronique nationale, créé par une banque centrale mais fonctionnant sur un système de registre distribué. Cette monnaie électronique servirait de complément et d'alternative aux dépôts bancaires traditionnels (le dollar, l'euro ou la livre électroniques côtoieraient leurs équivalents physiques). Selon les calculs des deux experts, si le stock de monnaie électronique représentait 30 % du PIB (émis en échange d'un montant équivalent

d'obligation d'État), un tel système permettrait une croissance de 3 % du PIB, grâce à « la réduction des taux d'intérêt réels, des distorsions de niveaux d'imposition et des coûts de transaction monétaire ». Mieux encore : cela contribuerait à la stabilisation de l'économie, « en donnant aux gouvernants un second outil pour mener leurs politiques en contrôlant soit le prix, soit la quantité de monnaie électronique émise », écrivent les auteurs. Il y aurait toutefois un inconvénient : « de véritables inquiétudes demeurent sur la manière de gérer convenablement les risques liés à la transition vers un régime monétaire et financier différent », admettent John Barrdear et Michael Kumhof.

De l'autre côté de la planète, des chercheurs de la banque centrale chinoise (également appelée Banque populaire de Chine) planchent sur le même sujet. En Chine, le Bitcoin connaît un succès exponentiel : entre le 1er mai et le 1er octobre 2016, le pays a concentré presque 95 % des échanges mondiaux de Bitcoins (sur ses trois plateformes dominantes, OKCoin, Huobi et Btcchina[39]). En 2013, son utilisation par les institutions financières avait pourtant été interdite par la banque centrale, mais devant le succès croissant du Bitcoin, la Banque populaire de Chine a lancé dès l'année suivante un groupe de réflexion chargé d'explorer les bénéfices des monnaies numériques et de concevoir sa cryptomonnaie souveraine (c'est-à-dire émise et contrôlée par la banque centrale). « Le développement d'un prototype est en cours[40] », a confirmé mi-novembre 2016 Yao Qian, le directeur de cette équipe de recherche, dans une interview au journal *Shanghai Securities News*.

Certaines banques centrales ont déjà commencé à expérimenter de tels systèmes. Mi-novembre 2016, celle de Singapour est devenue la première à annoncer officiellement la création de sa propre monnaie numérique. Celle-ci sera testée dans un système blockchain de paiement interbancaire (en partenariat avec la bourse locale et huit autres banques). « L'objectif est de simplifier les processus de paiement et de réduire les coûts de transaction[41] », a annoncé le directeur de l'institution, Ravi Menon, selon Bloomberg. Mi-juin, la Banque centrale du Canada avait déjà lancé, plus discrètement, une initiative similaire, révélait un article du magazine américain *Forbes*[42]. La Banque du Canada a mené des recherches sur la création d'une version électronique du dollar canadien sur la blockchain (le « Cad-Coin »), qui serait utilisée dans le cadre d'opérations entre institutions financières (en collaboration notamment avec le consortium R3). En Suède, la vice-gouverneure de la Banque de Suède, Cecilia Skingsley, a évoqué un projet plus ambitieux encore : la création « d'e-couronnes » (version électronique de la monnaie suédoise), utilisables par le grand public dans ce pays où la quasi-totalité des transactions se règle déjà de manière électronique, par carte bancaire (le liquide est devenu quasi obsolète). « Aurons-nous prochainement des e-couronnes dans notre e-portemonnaie, aussi naturellement que nous avons maintenant du liquide dans notre portefeuille ? Moins les Suédois utilisent de billets et de pièces, plus il semble clair que la banque centrale de Suède doit se demander si elle doit émettre une monnaie électronique en complément de la monnaie que nous utilisons aujourd'hui[43] », a ainsi déclaré Cecilia Skingsley lors d'une conférence sur les fintechs organisée à Stockholm mercredi 16 novembre.

Cet enthousiasme précoce est loin d'être partagé au siège de la Banque centrale européenne (BCE), où la méfiance domine encore envers les blockchains et les cryptomonnaies. La note publiée le 12 octobre 2016 par le président de la BCE, Mario Draghi, le prouve : « La BCE reconnaît que les

progrès technologiques permis par les registres distribués qui sous-tendent des moyens alternatifs de paiement, comme les monnaies virtuelles, ont la capacité d'accroître l'efficacité, l'étendue et la diversité des méthodes de paiement et de transfert. Mais les législateurs européens doivent faire attention à ne pas promouvoir l'usage de monnaies numériques privées comme moyens alternatifs de paiement, car elles ne sont pas légalement des monnaies, ni des moyens de paiement officiels émis par les banques centrales ou d'autres autorités publiques[44]. » Le président de la BCE liste ensuite une série de problèmes soulevés par les monnaies virtuelles : d'abord, « la volatilité associée aux monnaies virtuelles, qui est plus élevée que celles des monnaies émises par des banques centrales », ensuite « les possesseurs de monnaie virtuelle n'ont aucune garantie qu'ils pourront l'échanger dans le futur contre des biens, des services ou une monnaie légale », enfin « si les acteurs économiques étaient nettement plus nombreux à faire confiance aux monnaies virtuelles, cela pourrait en principe remettre en cause le contrôle des banques centrales sur la quantité de monnaie disponible, avec des risques sur la stabilité des prix. » En résumé, la BCE n'a pas envie de perdre la main sur la monnaie européenne.

Des devises virtuelles pourraient en effet potentiellement remettre en cause le monopole de l'institution sur la monnaie dans la zone euro, et permettre à certains pays membres de s'émanciper partiellement des règles et contraintes fixées par la BCE (notamment budgétaires). C'était l'idée d'un farouche adversaire de la BCE, le tempétueux économiste grec Yanis Varoufakis. En février 2014, un an avant de devenir ministre des Finances de la Grèce, dans le gouvernement de gauche radicale Syriza, Yanis Varoufakis évoquait sur son blog la possibilité, pour les pays du Sud de la zone euro, de « créer leur propre système de paiement, garanti par des taxes à venir et libellé en euros. […] Ils pourraient utiliser un algorithme de type Bitcoin pour créer un système transparent, efficace et sans coût de transaction[45] ». L'économiste avait appelé cette nouvelle monnaie FT-Coin (pour « futures taxes »). Il concluait ainsi sa réflexion : « Le design [du Bitcoin] peut être utilisé de manière profitable pour aider les pays membres de la zone euro à créer un système de paiement électronique libellé en euro, qui les aident, au moins à moyen terme, à surmonter l'asphyxie des pressions déflationnistes », imposées par les règles de la zone euro. Le FT-Coin n'a finalement jamais vu le jour. Mais cette idée est la preuve que la blockchain est un outil qui peut servir des visions politiques radicalement opposées, être mis à profit par les banques centrales tout comme par ceux qui veulent s'émanciper de leur tutelle.

Mutuelles décentralisées et assurance automatique

Le secteur de l'assurance est un de ceux qui s'est le plus intéressé à la technologie blockchain. Pour les assureurs et leurs clients, elle présente plusieurs avantages. Le premier est la transparence : elle permet la constitution de registres de données consultables par les différentes parties et impossibles à modifier, où peuvent être enregistrés les conditions contractuelles et l'historique des déclarations de sinistres et des demandes de remboursement. Le second est l'automatisation des remboursements, grâce à des *smart contracts* inscrits sur une blockchain, qui garantissent le versement immédiat d'une certaine

somme si un accident se produit et est détecté par un capteur connecté qui déclenche l'opération. Enfin, en théorie, la blockchain pourrait même permettre la désintermédiation de l'assurance par la constitution d'authentiques mutuelles cogérées par les adhérents (ou d'assurances pair à pair), selon des règles inscrites dans des *smart contracts*. Plus besoin alors de groupe mutualiste pour assurer la récolte des cotisations et le versement des remboursements aux conditions fixées : tout serait géré de manière transparente et automatisée sur la blockchain. Ne croyez pas qu'il s'agit là de fantasmes : tous ces cas d'usage font l'objet de recherches et d'expériences, bien concrètes, de la part de start-up et des départements d'innovation des grands assureurs, tous convaincus que la blockchain ouvrira une nouvelle page dans le secteur.

Partage sécurisé des données des assurés

En matière de transparence des données pour commencer, la société Blem, spécialisée dans les systèmes informatiques pour les réassureurs, a ainsi lancé un produit qui utilise la blockchain pour conserver un historique de toutes les demandes de remboursement de clients. Il présente un avantage pour les assureurs, à qui il offre un système simple garantissant la traçabilité de tous les événements relatifs aux sinistres dont ils doivent s'occuper. En partageant ce registre commun, « assureurs et réassureurs peuvent ainsi diviser les coûts entre eux[46] », note un article du *Financial Times*. Mais le service est également intéressant pour les assurés, ainsi certains que l'assureur ne peut pas modifier les données qu'ils ont inscrites dans leurs réclamations. La gestion des données, sécurisées sur la blockchain, pourrait donner naissance à de nouveaux modèles économiques. « Le secteur de l'assurance va être considérablement impacté par l'afflux de données générées par les objets connectés. Les compagnies d'assurances pourraient proposer aux consommateurs de leur offrir de meilleurs tarifs si ces derniers les laissaient utiliser ces données », suggère l'expert suisse des fintechs, Nicolas Steiner. « Imaginons que j'habite à Londres et que je sois de passage en France. Je loue une voiture et souscris une assurance. Dans la blockchain, l'assureur pourrait avoir accès à mes informations de conduite à Londres. La blockchain offrirait alors un moyen de transférer en temps réel mes données personnelles de manière sécurisée en respectant la vie privée des utilisateurs[47] », relève-t-il.

Bientôt des assurances automatiques

Mais c'est surtout sur le concept d'automatisation de la police d'assurance et du remboursement que d'innombrables projets ont été menés. « Il existe aujourd'hui plusieurs cas d'usage d'automatisation, où l'assurance se régule en fonction d'un certain nombre d'informations qu'elle reçoit[48] », note le consultant Éric Lévy-Bencheton, spécialiste de la blockchain chez Keyrus. « Prenons par exemple l'assurance voyage », poursuit-il. « Il existe des contrats qui ne couvrent pas certaines villes ou certaines zones [jugées dangereuses par exemple]. Avec les smartphones, on peut savoir où chacun va. On pourrait donc

avoir des assurances directement évaluées en fonction du risque de l'endroit où l'on se rend. » La souscription sera accélérée et facilitée, ajoute Nicolas Steiner : « Avec mon téléphone, je pourrai cliquer pour m'assurer trois jours, presque en temps réel, si je suis en voyage quelque part », suggère-t-il. Autre exemple : la gestion des sinistres. « Sur des sinistres simples, on peut facilement capter de l'information et payer à l'assuré ce qui a été convenu dans le contrat. Par exemple, dans le cas d'un agriculteur qui s'assure contre un ensoleillement trop fort ou au contraire pas assez important, on pourrait avoir un *smart contract* automatique qui vérifie auprès d'un tiers de confiance, qu'on appelle un "oracle", les conditions météorologiques (Météo France dans ce cas) », imagine Éric Lévy-Bencheton.

Des grands groupes comme Axa, Allianz et IBM ont tous planché, ces derniers mois, sur ces possibilités d'automatisation. « Ça nous intéresse[49] », confirme Laurent Benichou, directeur de l'innovation et de la prospective chez Axa. « On pourrait regarder les cas où la souscription pourrait être simple et où la vérification du sinistre pourrait être faite de façon automatique, sans que la personne ayant souscrit le contrat n'ait à faire de démarche. Le consommateur serait remboursé sans même faire de déclaration de sinistre », précise-t-il. Pour un de leurs clients, les équipes d'IBM France ont développé un prototype dédié aux agriculteurs : « Nous avons imaginé une assurance qui les dédommagerait en cas de catastrophe naturelle[50] », raconte Luca Comparini, le responsable blockchain d'IBM France. « Un *smart contract* exécuterait le dédommagement, et serait déclenché sur la base d'informations fournies soit par des capteurs sur le terrain, soit par un oracle. » Dans l'expérience menée par IBM, l'oracle choisi était Weather Channel, la plus grande infrastructure mondiale de données météo (rachetée par IBM en octobre 2015). « Ainsi, on peut récupérer des informations sur la pluviométrie localisée dans un territoire, dans l'espace et le temps, et fournir ensuite une réponse binaire [oui ou non] qui permet de déclencher le *smart contract* », précise Luca Comparini. Le géant allemand de l'assurance, Allianz, s'est lui aussi penché sur les catastrophes naturelles et a lancé en juin 2016 « Allianz Risk Transfer », en partenariat avec Nephila : un produit blockchain dédié aux investisseurs exposés aux risques de catastrophe naturelle.

Ce type d'assurance automatique, appelé assurance paramétrique, existait avant la blockchain, fait remarquer Laurent Benichou, d'Axa, qui a choisi de ne pas se focaliser sur l'agriculture, trop complexe à gérer : « Ça mobilise beaucoup de données, et ce n'est pas facile d'avoir une information fournie par un oracle, suffisamment précise et fiable pour déclencher un paiement », estime-il. Axa s'est donc plutôt intéressé à d'autres usages d'assurance paramétrique, plus simples. « Par exemple l'assurance retard d'avion », explique Laurent Benichou, qui cite le prototype Insureth, basé sur la blockchain Ethereum. « Ce service se branche à une base de données des heures d'arrivée réelle des avions. Ensuite, on compare à l'heure d'arrivée théorique, on déduit le niveau de retard et au-delà de 4 ou 5 heures, par exemple, on déclenche l'indemnisation », explique-t-il. Bien d'autres applications sont envisagées par Axa, comme l'assurance antipollution. « Il existe une start-up israélienne, BreezoMeter, qui indique la qualité de l'air dans plusieurs pays du monde. Si on se branchait à leur système, on pourrait déclencher un paiement automatique quand le niveau de pollution atteint un certain niveau. Si vous êtes asthmatique,

vous pourriez être dédommagé quand vous ne pouvez pas aller au travail, que vous êtes obligé de prendre un taxi ou d'acheter un masque antipollution », détaille Laurent Benichou.

L'assurance décès est aussi dans le viseur des assureurs. Elle fait partie des quelques prototypes développés de manière collaborative par l'initiative sectorielle Labchain, menée par la CDC (notamment avec Axa). « Avoir des démarches simplifiées dans ce genre de situations, c'est précieux » commente Laurent Benichou. Dans le prototype imaginé par Labchain, le bénéficiaire serait indemnisé automatiquement dès l'enregistrement du décès. « Malheureusement, ça ne pourra pas être commercialisé tel quel, car le registre de l'État ne semble pas mis à jour assez régulièrement par les mairies pour que l'application soit viable aujourd'hui », regrette Laurent Benichou. « On se met en ordre de bataille pour être prêts au moment où le fichier sera mis à jour, à haute fréquence et de façon sûre », ajoute-t-il. L'assurance automobile pourrait elle aussi être impactée. Selon un rapport du cabinet Capgemini, « l'utilisation de *smart contracts* dans le secteur de l'assurance automobile personnelle pourrait faire économiser 21 milliards de dollars de coûts [au niveau mondial et par an] grâce à l'automatisation et à la réduction des frais engagés dans la gestion des déclarations[51] ». Un chiffre gigantesque, extrapolé à partir d'une étude du secteur de l'assurance auto au Royaume-Uni. « Grâce aux économies faites par les assureurs, les consommateurs seraient en droit d'attendre des primes d'assurance réduites », ajoutent les auteurs. En effet !

Des véritables mutuelles pair à pair

Enfin, certaines start-up commencent à développer des projets, plus révolutionnaires encore, d'assurance pair à pair (ou décentralisée) : des coopératives d'assurés qui se couvrent mutuellement. En d'autres termes, de pures mutuelles, où les *smart contracts* garantissent la couverture et le versement des remboursements, en lieu et place du groupe mutualiste. C'était l'ambition de Wekeep.io, un projet de recherche développé par le Français Adrian Sauzade (également fondateur de Czam), vainqueur d'un hackathon organisé en juillet 2015 par la compagnie d'assurances Maif, avec son application et son site Web d'assurance décentralisée. « L'idée était de considérer l'assurance comme du pari et de proposer aux particuliers de se porter caution collectivement pour un risque que je veux assurer[52] », résume-t-il. « C'est du « crowdassurance » [assurance participative]. Si ceux qui acceptent d'assurer ont assez mutualisé le risque, à la fin, ils sont gagnants [s'ils ont assuré suffisamment de gens pour que la grande majorité des assurés n'ait pas de problème et ne demande pas de remboursement]. C'est le principe des Lloyd's de Londres au XVII^{e} siècle, qui a donné naissance aux assurances : les gens pariaient sur des bateaux qui réussissaient à arriver aux États-Unis ou coulaient. Certains pariaient contre leur propre bateau, alors ils pouvaient récupérer une partie de leur mise si le navire sombrait. L'assurance, c'est du pari », rappelle Adrian Sauzade. Le concept de Wekeep.io a suscité l'enthousiasme dans le secteur. Mais, trop complexe, il n'est pas réalisable en l'état.

Adrian Sauzade développe donc aujourd'hui un mécanisme plus simple de mutuelle pair à pair, qui fonctionnerait avec un séquestre en Bitcoins (une sorte de pot commun), dont seraient retirées les primes,

déclenchées soit par un système de vote, soit par un système de flux (de manière automatique selon des conditions préétablies et inscrites dans le code). Mais il n'est pas évident pour un nouvel entrant de réussir à percer. « Il y a trois problématiques majeures. D'abord, la mutualisation du risque, qui doit être assez dispersé. Ensuite, l'antisélection : quand quelqu'un demande un contrat d'assurance, il va vouloir cacher les informations qui vont faire monter le montant de sa prime. Enfin l'aléa moral : tu peux ne pas faire attention à tes affaires parce que tu es assuré. C'est pour ça qu'il y a une franchise et des systèmes de bonus-malus. Tout cela est difficile à surmonter, quand tu crées une assurance à partir de rien », admet Adrian Sauzade. Mais l'idée intéresse les grands assureurs, qui l'ont tous ou presque invité à leur expliquer son fonctionnement.

Une autre start-up hexagonale, Stratumn, a elle aussi travaillé sur un prototype baptisé LenderBot et dévoilé mi-juillet 2016, en partenariat avec le cabinet Deloitte. Raccordée à Facebook Messenger, LenderBot est une offre d'assurance pair à pair pour les objets de valeur que des amis se prêtent entre eux. Les utilisateurs indiquent un certain nombre d'informations dans un petit logiciel connecté à Facebook (identité des participants, valeur de l'objet prêté, durée du prêt, coût de l'assurance). Ces informations sont transmises à Stratumn, qui les inscrit dans la blockchain sous forme de hash (l'empreinte digitale unique, alphanumérique), et crée un *smart contract* fidèle aux conditions précisées. « Le prototype fonctionne, nous le faisons tourner chez nous et avec notre partenaire Deloitte, qui l'utilise pour ses démonstrations auprès de grands assureurs[53] », indique François Dorléans. Il ne faut pas traîner, car la concurrence est féroce. À l'étranger, plusieurs autres jeunes pousses se sont aussi lancées dans des projets d'assurances pair à pair et participatives, comme Friendsurance (en Allemagne), Lemonade (États-Unis) ou Guevara (Royaume-Uni), sans toutefois utiliser de blockchain.

---

*1. Comme certains produits dérivés qui ont causé la crise de 2008, par exemple.

*2. IP : Internet Protocol.

*3. Prêt accordé à une entreprise par plusieurs banques.

*4. Tarifs à l'automne 2016.

CHAPITRE 5

Une vraie économie du partage

La créature a échappé à son maître. Comme le monstre du Dr Frankenstein, dans le roman de Mary Shelley, le Web, inventé par le professeur britannique Tim Berners-Lee en 1990, a fini par effrayer celui qui lui a donné naissance. Conçu initialement pour faciliter l'échange d'information entre les scientifiques du monde entier, le Web a réussi bien au-delà de ses ambitions initiales, bouleversant à jamais l'accès à la connaissance, à la communication et au commerce. Mais vingt-six ans plus tard, le réseau a un visage bien différent de celui qu'imaginait son inventeur. « Ça a été génial, mais l'espionnage, le blocage de sites, le reformatage du contenu produit par les internautes, la redirection vers les mauvais sites… tout cela sape complètement l'esprit originel qui était d'aider les gens à créer[1] », a-t-il déclaré lors du premier « sommet du Web décentralisé » à San Francisco, en juin 2016, comme le rapporte un article du *New York Times*. Avec quelques autres informaticiens pionniers (dont Vincent Cerf, co-inventeur de TCP/IP, un des protocoles de transfert de données sur Internet), Tim Berners-Lee a ainsi décidé de se mobiliser pour imaginer une nouvelle phase du Web, où ce dernier serait plus décentralisé et plus respectueux de la vie privée de ses utilisateurs.

Le virage jacobin d'Internet

La centralisation quasi monopolistique est en effet devenue la règle dans l'économie numérique. Dans tous les services qui mettent en relation l'offre et la demande, un acteur dominant, voire ultradominant, a émergé : les moteurs de recherche et la messagerie (Google), le commerce électronique (Amazon), les réseaux sociaux (Facebook), le Web mobile et la vente de musique (Apple), la mise en relation avec des chauffeurs (Uber), la location de logement (Airbnb)… Sur le Net, le marché a tendance à constituer lui-même ces positions de force (que l'on appelle des « monopoles naturels ») par un

mécanisme facilement compréhensible : les consommateurs se rassemblent spontanément sur la plateforme où l'offre (de sites référencés, d'amis membres du réseau, de chauffeurs ou de loueurs) est la plus large, tandis que l'offre (annonceurs sur Google ou Facebook, chauffeurs sur Uber, loueurs sur Airbnb) se concentre, elle aussi, sur la plateforme où les clients sont les plus nombreux. Résultat, la concurrence disparaît peu à peu, un grand gagnant émerge et peut ensuite faire la loi sur son secteur. C'est ainsi que les Gafa (Google, Amazon, Facebook, Apple) sont devenues immensément riches : toutes classées parmi les dix plus grands groupes mondiaux, elles cumulaient une capitalisation, à elles quatre, de 1 727 milliards de dollars au 31 mars 2016 (soit plus que le PIB de toute l'économie brésilienne par exemple, ou l'équivalent de 70 % du PIB de l'économie française, selon les estimations 2016 du FMI). C'est aussi la perspective d'un succès similaire qui explique l'incroyable valorisation d'Uber. La société, non cotée en bourse pour l'instant, était déjà estimée par ses investisseurs à plus de 62,5 milliards de dollars en juin 2016, alors même qu'elle n'avait toujours fait aucun bénéfice. Ces derniers font le pari qu'Uber écrasera tous ses rivaux et deviendra le roi incontesté du transport à la demande dans le monde, atteignant une position de quasi-monopole qui lui permettra alors de devenir extrêmement rentable, pour longtemps.

Que toutes ces sociétés s'enrichissent n'est pas problématique en soi. Mais dans une économie de marché, les monopoles ont tendance à aboutir à une détérioration de l'offre, à une hausse des tarifs ou à des pratiques abusives imposées au consommateur (ainsi, quand Google décide de déréférencer un site, il signe son arrêt de mort, ce qui confère au groupe californien un pouvoir démesuré sur ceux avec lesquels il négocie). « Le problème est la domination d'un seul moteur de recherche, d'un seul grand réseau social, d'un seul Twitter pour le microblogging », résumait Tim Berners-Lee lors de la conférence de San Francisco.

Sur le Web, cette concentration, qui se traduit par une centralisation des données des utilisateurs dans les serveurs de Google, Facebook, Amazon ou Uber, a des défauts supplémentaires : elle facilite l'espionnage (comme l'illustre le scandale Snowden, qui nous a appris la surveillance de masse du Net par la NSA), le hacking (pensons à celui des 500 millions de messageries Yahoo, dévoilé en novembre 2016) ou la censure (en Chine par exemple).

Décentraliser Internet

Heureusement, cette situation n'est pas une fatalité et des solutions existent pour décentraliser l'économie numérique. Devinez quelle est celle qui a émergé des discussions du sommet du Web décentralisé, à San Francisco ? Les « systèmes de registres comme ceux utilisés par les cryptomonnaies », rapporte le journaliste du *New York Times*, Quentin Hardy. En d'autres termes, la blockchain. Dans le secteur des cryptomonnaies, nombreux sont ceux qui voient en elle un remède inespéré pour changer les rapports de force sur le Web, contester ces « monopoles naturels » et remettre le pouvoir entre les mains des internautes.

Pour Pierre Noizat, fondateur de Paymium, « la décentralisation des serveurs est un enjeu majeur économique et démocratique. Économique d'abord, car aujourd'hui, un serveur central (toujours américain) capture toutes les données dans chaque secteur : Amazon, Apple, Uber, Google… La valeur ajoutée est ainsi aspirée dans la Silicon Valley. Politique ensuite, car ce mécanisme aboutit à un appauvrissement des classes moyennes. Il n'y a plus de redistribution par l'impôt, puisque ces entreprises font toutes de l'optimisation fiscale[2] », insiste-t-il. Pour cette raison, la blockchain et en particulier, pour Pierre Noizat, le Bitcoin, sont fondamentaux : « Ça permet de décentraliser la brique paiement. Dès lors, vous pouvez décentraliser le reste de l'application », explique-t-il. Tous les services numériques, d'Amazon à Uber, peuvent être réinventés en version décentralisée, en utilisant la blockchain, comme nous allons le voir dans les pages qui suivent. C'est là le véritable défi du Bitcoin et des autres cryptomonnaies : « L'enjeu du Bitcoin, c'est la décentralisation de l'économie numérique. Pour certains, le Bitcoin menacerait la souveraineté des États. Mais en réalité c'est l'inverse. Les États sont vassalisés par les serveurs installés dans la Silicon Valley. Le Bitcoin, au contraire, est un contre-pouvoir grâce auquel nous pouvons regagner de la souveraineté. » Capable de changer les rapports de force technologique et de redistribuer les cartes, la blockchain offre une seconde chance à Internet.

Cette réinvention d'un Web décentralisé est l'ambition de Vitalik Buterin, le jeune fondateur d'Ethereum, une blockchain conçue pour donner naissance à des millions « d'applications distribuées » (d-App), qui s'attaqueront aux grands monopoles du Net en recréant tous les services en ligne en version pair à pair. Dès 2013, avant même le lancement de son projet, le jeune informaticien canadien soulignait sur son blog le bénéfice qu'apporteraient à l'économie des « entreprises décentralisées » (des organisations qui reposeraient sur l'action d'applications décentralisées). « Dans quelles industries des entreprises décentralisées […] seraient-elles capables […] d'apporter une vraie valeur ajoutée à la société ? […] D'abord, il y a les monopoles naturels. Pour certains services, cela n'a pas de sens de mettre en compétition des centaines d'offres en même temps. [...] Mais, si les prestataires de ces services ne sont pas sous la pression d'un marché compétitif, qui les contrôle ? Qui s'assure qu'ils font payer un prix honnête pour leurs services, et qu'ils n'établissent pas des tarifs monopolistiques 1 000 fois supérieurs à ce que coûte véritablement ce qu'ils produisent ? En théorie, une entreprise décentralisée peut être conçue pour que ceux qui fixent un prix ne soient pas tentés de faire cela[3]. » Cette prophétie est en passe de devenir réalité. En Israël, aux États-Unis, en France ou encore au Royaume-Uni, d'innombrables start-up ambitionnent de réinventer toute l'économie numérique à la sauce blockchain. Misant pour certaines sur le Bitcoin, pour d'autres sur Ethereum, elles veulent remettre consommateurs et producteurs (de biens ou de services) en relation directe, grâce aux applications décentralisées. Cette révolution en germe pourrait non seulement bousculer les géants du Web dans chaque domaine où ils ont établi leur emprise, mais aussi permettre de réinventer toute la chaîne de valeur dans le secteur de la culture, pour redonner le pouvoir aux artistes. Enfin, elle ambitionne de changer à jamais notre manière de miser sur l'avenir, en bouleversant le système des paris, des jeux et même des sondages.

Objectif : bousculer les géants du Web

L'économie numérique a connu quatre grandes vagues, qui ont chacune fait émerger leurs champions : d'abord celle des moteurs de recherche, des messageries et du commerce électronique, incarnée par les géants Google (fondé en 1998) et Amazon (dès 1994) ; ensuite, celle de réseaux sociaux et de l'Internet « 2.0 » (participatif), symbolisée par Facebook ou Twitter (respectivement créés en 2004 et 2006) ; puis, celle de l'économie collaborative (ou « du partage »), dont les fers de lance ont été Airbnb (2008) et Uber (2009) ; enfin, celle du cloud ou de « l'informatique dématérialisée », un marché juteux que se sont partagé des géants déjà installés (Amazon, Google, Microsoft et IBM) et quelques nouveaux entrants (Dropbox, créé en 2008). Une cinquième est peut-être en train de se former avec la blockchain, qui va réinventer tous les services nés des quatre premières vagues en version décentralisée, sans intermédiaire.

Le commerce électronique en mode pair à pair

Le plus ancien géant d'Internet, Amazon, est aussi le premier à avoir été concurrencé par un projet fondé sur la blockchain : OpenBazaar, un marché en ligne entièrement pair à pair, lancé en septembre 2014 par l'Américain Brian Hoffman. « C'est un réseau de gens qui, partout dans le monde, commercent directement entre eux en Bitcoins, en utilisant un programme *open source* qu'ils peuvent installer gratuitement sur leurs ordinateurs[4] », explique le fondateur. « Aucune autorité centrale ne contrôle le réseau ni ne prend de pourcentage sur les ventes. OpenBazaar n'a ni commission ni capacité d'interdire une vente. Ce système permet le libre-échange sur Internet. » Plus de 300 000 personnes ont déjà téléchargé l'application et plusieurs milliers l'utilisent pour acheter les produits les plus divers (pots de miel, Lego de collection, T-shirts, matériel informatique…). « Les articles qui semblent les plus populaires sont les sauces pimentées et les livres », juge Brian Hoffman, bien qu'il n'ait aucune statistique sur les ventes (puisqu'il ne contrôle pas le système).

Un projet de hacker, ensuite rentré dans le rang

L'histoire du projet est étonnante. Ses racines remontent aux tout premiers sites de e-commerce illégaux qui ont, de manière pionnière, proposé des paiements en Bitcoin (en raison du relatif anonymat offert par la devise). Hébergée sur le Dark Web, l'Internet caché, la plateforme Silk Road (fondée en février 2011) a connu un succès fulgurant comme marché noir du crime : drogues, armes et faux papiers s'y échangeaient en toute discrétion contre des paiements en Bitcoins, jusqu'à la fermeture du site par le FBI en octobre 2013. Cette sulfureuse initiative a beaucoup nui à la réputation du Bitcoin, associé pour longtemps à la criminalité dans l'esprit du grand public. Après la fermeture de Silk Road, le développeur anglo-iranien Amir Taaki, un hacker anarchiste de talent, a créé, à l'occasion du hackathon Bitcoin de Toronto (une compétition de codage), l'ancêtre d'OpenBazaar : le site Dark Market, qui voulait, comme Silk Road, permettre l'échange de produits illicites. Mais pour empêcher que le FBI puisse fermer l'application, Amir Taaki l'avait conçu de manière décentralisée : Dark Market était un programme installé chez chacun de ses utilisateurs, capables de mener leurs échanges entre eux en direct, sans intermédiaire. Il n'y avait alors plus de serveur à couper, ni d'organisateur à arrêter. « Taaki a décidé de ne pas poursuivre le projet, je m'en suis inspiré mais je l'ai modifié et je lui ai donné un autre nom, OpenBazaar, et une autre vision », raconte Brian Hoffman. « Celle du Dark Market était centrée sur les produits illicites, mais c'était une perspective trop étroite. Le pair à pair peut bénéficier à tout le monde et la vision d'OpenBazaar est de mettre le libre-échange à la portée de tout un chacun », ajoute-t-il.

De vrais atouts

L'application possède quelques réels avantages par rapport aux plateformes traditionnelles de commerce électronique (Amazon, eBay, Le Bon Coin, etc.). D'abord, l'absence de commission, qui rend le service compétitif pour les vendeurs face à Amazon (qui prélève 7 à 20 % du montant de la vente selon les produits) ou eBay (qui en retire 7,5 %). Ils peuvent ainsi proposer leurs biens moins cher, ce qui bénéficie aussi aux clients. Ensuite, l'assurance de rester maître de ses données personnelles : « Une entreprise comme Amazon a une quantité incroyable d'informations sur les clients et leurs habitudes d'achat. Sur OpenBazaar, les données sur les acheteurs, les vendeurs et les ventes ne sont transmises à aucune entreprise ou organisation, elles sont seulement partagées entre les deux parties de la transaction », souligne Brian Hoffman. Troisième atout : l'utilisation du Bitcoin pour régler les transactions, qui garantit une plus grande maîtrise de ses informations personnelles (pas besoin de s'identifier), une meilleure sécurité (pas de numéro de carte de crédit à hacker) et fait disparaître les commissions sur les transactions prélevées par les compagnies de carte de crédit ou par Paypal. Enfin, OpenBazaar offre un dernier avantage, à double tranchant, à ses adeptes : il y règne une liberté totale d'achat et de vente. « OpenBazaar n'impose aucune restriction. Si un vendeur n'a pas le droit de vendre tel bien ou service sur d'autres plateformes, il peut utiliser OpenBazaar. L'application n'a, de plus, aucune limite géographique et peut être utilisée n'importe où », ajoute le fondateur. Ce point laisse

perplexe sur la légalité du service. Mais Brian Hoffman reporte la responsabilité sur les utilisateurs : « Il appartient aux vendeurs de s'assurer qu'ils opèrent dans le respect de la législation de leur juridiction. » Lui-même n'a aucun moyen de faire la police sur l'application. « C'est un réseau de gens qui utilisent un logiciel sur leur ordinateur pour se connecter entre eux. La seule manière de les empêcher de vendre des choses illégales, c'est de prendre le contrôle de leur ordinateur et de fermer leur boutique », précise-t-il. Brian Hoffman n'est pas inquiet : « Nous espérons que l'utilisation d'OpenBazaar reflétera la manière dont la société fait du commerce – presque entièrement de manière légale et positive, avec seulement une petite portion d'utilisateurs qui enfreignent la loi. »

À ce jour, OpenBazaar reste microscopique par rapport à son rival Amazon (qui servait environ 304 millions de clients fin 2015, soit 1 000 fois plus que le nombre de personnes ayant téléchargé OpenBazaar) ou par rapport à ses autres concurrents, eBay ou Le Bon Coin. Mais le potentiel de l'application a permis à Brian Hoffman de lever un million de dollars en juin 2015 pour assurer son développement, auprès de fonds de capital-risque reconnus dans la Silicon Valley (Andreessen Horowitz, qui avait investi dans Twitter ou LinkedIn, et Union Square Ventures, qui avait misé sur Twitter et Tumblr). Cet argent a été placé dans la société OB1, créée par Brian Hoffman avec quelques associés. Celle-ci veille au développement de l'application OpenBazaar et prévoit, à terme, de vendre des services aux utilisateurs du réseau (c'est ainsi que Brian Hoffman compte gagner de l'argent). Le fondateur voit loin et perçoit son projet comme l'avant-garde d'un vaste mouvement de décentralisation du commerce en ligne : « Amazon, eBay et les autres géants du e-commerce ont des millions d'utilisateurs et une longue ancienneté, qui leur a permis de bâtir des services compétitifs pour leurs clients. L'émergence du commerce en pair à pair sur OpenBazaar n'a que quelques mois. Mais la suppression de l'intermédiaire, et de sa commission de 10 à 15 %, ainsi que l'amélioration de la sécurité et du respect de la vie privée, sont des atouts très attirants pour les acheteurs et les vendeurs. Nous espérons que les avantages du commerce pair à pair sont suffisamment substantiels pour que, petit à petit, les gens abandonnent le système de e-commerce centralisé et contrôlé pour ce modèle ouvert et décentralisé. OpenBazaar est le logiciel qui mènera cette transition. Nous n'arrêterons pas de le développer tant qu'il ne comptera pas plusieurs millions d'utilisateurs partout dans le monde », promet-il.

Nouvelle chance pour les réseaux sociaux décentralisés

La blockchain réussira-t-elle là où d'autres pionniers de la décentralisation ont échoué ? Dès 2010, alors que seule une poignée de cryptographes avait entendu parler du Bitcoin et compris l'intérêt de son fonctionnement en blockchain, certains imaginaient déjà des recours pour permettre aux internautes de reprendre la main sur leurs données personnelles. Choqués par la mainmise de Facebook sur ce trésor numérique, quatre étudiants new-yorkais ont alors lancé diaspora*, le premier réseau social décentralisé. S'il n'utilisait pas de blockchain, l'esprit du projet et ses principes de fonctionnement étaient très proches. Cette application, dont le code *open source* a été diffusé en septembre 2010, permettait à ses

membres de s'inscrire sur un des serveurs existants ou de créer leur propre serveur pour garder le contrôle de leurs données ou le déléguer à un serveur de confiance. L'ensemble constituait un réseau de multiples nœuds[*1], sur lesquels personne ne pourrait exercer de contrôle total, ce qui assurait une meilleure protection contre la surveillance que les réseaux sociaux traditionnels aux serveurs centralisés. Accueilli avec un grand enthousiasme, diaspora* avait réussi à attirer, en juin 2010, près de 200 000 dollars d'investissement auprès de 6 479 contributeurs, sur la plateforme de financement participatif Kickstarter (un record à l'époque). Mais le réseau s'est heurté à des difficultés techniques et à des problèmes personnels des fondateurs, qui ont quitté le navire en août 2012. Depuis, il existe toujours, grâce aux efforts d'utilisateurs bénévoles. Fin novembre 2016, il comptait 657 535 inscrits, dont seulement 60 026 actifs dans les six derniers mois[5]. On est bien loin des 1,79 milliard de membres actifs sur Facebook (au 30 septembre 2016)… Utopie rattrapée par la réalité, diaspora* n'a donc jamais atteint son objectif initial d'offrir au grand public une alternative décentralisée fiable à Facebook. Le défi était trop grand, comme l'explique le journaliste du site américain Slate.com, Will Oremus : « Quel que soit le nombre de personnes qui rejoignaient l'application, elle faisait toujours figure de ville fantôme comparée à Facebook. […] C'est affreusement difficile de construire un réseau social avec de meilleures caractéristiques que Facebook, surtout quand la principale chose qui importe aux gens dans un réseau social est que tous leurs amis soient dessus[6]. »

Les enfants de diaspora*

Aujourd'hui, plusieurs applications blockchain reprennent pourtant le flambeau de diaspora* et promettent à leur tour de concevoir des réseaux sociaux décentralisés, imperméables à la censure, où les internautes seraient maîtres de leurs données et libres de s'exprimer. Fondée en 2014, la start-up américaine Synereo a ainsi l'ambition de créer un réseau social décentralisé, possédé et géré par ses utilisateurs, et conçu pour leur permettre de mettre en avant les contenus qui méritent selon eux de l'attention. En mars 2015, elle a lancé une première levée de fonds auprès des internautes, suivie d'une seconde en septembre 2016, qui lui a permis de récolter près de 4,7 millions de dollars pour développer sa propre blockchain[*2]. Grâce à celle-ci, chaque utilisateur pourra garder un contrôle total sur ses données et informations personnelles, et décider auprès de qui elles doivent être partagées. Synereo devrait mettre en ligne son service fin 2017.

Plusieurs autres projets ont été lancés courant 2016, dont celui de la start-up américaine Steemit. Présenté en mars dans un article de recherche (*white paper*) et lancé en juin, Steemit se présente comme une version décentralisée de Reddit. Peu connu en France, ce site de partage de liens populaires auprès des utilisateurs a connu un grand succès et reste le 26e site le plus utilisé au monde (et le 8e aux États-Unis). Steemit ajoute deux caractéristiques à celles de son prestigieux ancêtre. D'abord, la décentralisation : le contenu sous forme de texte est enregistré dans les nœuds de la blockchain Steem, dont le code est *open source*. Les images ou vidéos en revanche doivent être enregistrées sur d'autres sites Web (et apparaissent par un système de liens). Mais le vrai apport de Steemit n'est pas là : quand

les membres du réseau votent pour distinguer un contenu qu'ils jugent de qualité (comme avec un « like » sur Facebook), son auteur reçoit alors une gratification dans la cryptomonnaie du réseau (« Steem »). Les utilisateurs sont aussi récompensés quand ils partagent ou commentent des contenus. Ce système a permis à Steemit de connaître un succès fulgurant : fin octobre 2016, avec à peine 5 mois d'existence, la start-up comptait déjà 100 000 utilisateurs, auprès desquels elle avait distribué l'équivalent de 4 millions de dollars, selon le magazine américain *Rolling Stone*[7]. Sur le même principe, un autre réseau social, Yours (anciennement nommé Datt), est en cours de développement et devrait être lancé auprès du grand public courant 2017. Sur Yours, les membres pourront recevoir une sorte de pourboire, en Bitcoins, de la part des autres utilisateurs, s'ils ont produit ou partagé un contenu de qualité. Le 3 mai 2016, journée mondiale de la liberté de la presse, un troisième projet du même genre, développé lui avec la blockchain Ethereum, était dévoilé : Akasha. Ce « réseau de médias sociaux de nouvelle génération », ainsi qu'il se définit, fonctionnera comme une plateforme de blog résistante à toute forme de censure, son caractère décentralisé le rendant indépendant des serveurs.

Résister à la censure

La résistance à la censure pourrait bien être le facteur clé qui fera décoller l'utilisation de ces services. Dans les pays exerçant un contrôle fort sur les médias et Internet, ils offriraient des espaces de liberté précieux. Un État peut difficilement agir sur de tels systèmes, car il n'y a pas de serveur à fermer ni à espionner. La Russie, par exemple, a resserré son contrôle sur les réseaux sociaux depuis une loi, entrée en application en septembre 2015, qui impose aux firmes étrangères de stocker sur le sol national les informations personnelles des internautes russes. À l'automne 2016, l'agence de régulation des télécoms, Roskomnadzor, a bloqué l'accès au réseau social professionnel LinkedIn. Facebook et Twitter sont également dans le viseur des autorités. C'est dans ce contexte qu'a eu lieu, en novembre 2016, la conférence Bitcoin Russia à Moscou. Lors de cet événement, cyber.Fund, un groupe de développeurs russes qui a constitué une plateforme d'investissement décentralisée, a annoncé le lancement du premier réseau social russe décentralisé. Baptisé Voice et calqué sur le modèle de Steemit, ce réseau permettra, selon ses créateurs, « aux auteurs (blogueurs et journalistes) de publier leurs productions sans peur de la censure, tout en accédant à une audience plus large[8] ».

Dans le domaine des services de micro-blogging, comme Twitter, différentes tentatives ont été également menées. La première, qui semble avoir été abandonnée depuis, est Twister : un équivalent décentralisé de Twitter, inventé dès juin 2013 par le développeur brésilien Miguel Freitas, et reposant sur le protocole Bitcoin. Twister garantissait à ses utilisateurs le cryptage de leurs messages privés, une protection contre la censure (personne ne peut effacer les tweets ni supprimer les comptes) et un véritable anonymat (l'adresse IP des personnes connectées n'est enregistrée nulle part). Malheureusement, plus de trois ans plus tard, cette application n'a toujours pas de version grand public. Mais l'idée était bonne et d'autres développeurs ont commencé un projet similaire : Ethertweet, fonctionnant lui sur la blockchain

Ethereum. Un premier prototype, qui permet d'envoyer et de recevoir des messages de 160 caractères maximum, est téléchargeable, mais le service ne paraît pas encore très facile d'utilisation.

Quels que soient leur potentiel et leur niveau de maturité, tous ces nouveaux services de réseaux sociaux sur la blockchain posent un problème majeur que les développeurs devront prendre en compte : les informations inscrites sur une blockchain sont supposées être impossibles à effacer, ce qui veut dire que les posts sont permanents. Qui n'a pas déjà regretté avoir publié un peu trop rapidement sur un réseau social ? Ainsi, sur Steemit, plusieurs utilisateurs s'inquiétaient de ne pas pouvoir effacer leurs publications. Comme le disait Andrew, un membre italien du réseau : « Je n'aime pas l'idée que mes posts soient gravés dans le marbre à jamais[9]. » Or, dans l'Union européenne, une décision de la Cour de justice européenne, le 13 mai 2014, a garanti pour chacun le « droit à l'oubli ».

Uberiser Uber, Airbnb et les autres géants de « l'économie du partage »

En 2008-2009, alors que la crise financière plongeait le monde dans un marasme durable, plusieurs start-up californiennes ont amorcé un vaste mouvement de transformation de l'économie sur la base d'un concept qui avait semblé jusqu'alors difficilement compatible avec le capitalisme : le partage. En 2008, l'Américain Brian Chesky (27 ans à l'époque) lançait ainsi Airbnb, un site de location de logements entre particuliers. Un an plus tard, en 2009, son compatriote Travis Kalanick créait Uber, une application de mise en relation avec des chauffeurs indépendants. Dans les deux cas, ces jeunes entreprises, vite devenues gigantesques (Airbnb était valorisée 30 milliards de dollars en août 2016, Uber, 62,5 milliards de dollars en juin 2016), promettaient de bousculer l'ordre établi de secteurs très réglementés comme l'hôtellerie ou les taxis, en proposant à n'importe qui de se transformer, ponctuellement ou pour de bon, en entrepreneur individuel en mettant son bien (son appartement ou sa voiture) et éventuellement sa force de travail à la disposition de clients le temps de la prestation. Dans la foulée, de nombreuses autres jeunes pousses ont appliqué le concept à d'autres domaines comme la location de voiture entre particuliers (Drivy lancé en 2010, Ouicar en 2012) ou le financement participatif (Kickstarter en 2009, Kisskissbankbank en 2010). Prônant un même esprit collaboratif, cette nouvelle génération de plateformes en ligne de mise en relation entre clients et particuliers prestataires de services a été rassemblée sous la bannière d'« économie du partage » (*sharing economy*), un concept attribué au professeur de droit de Harvard Lawrence Lessig, qui l'aurait employé pour la première fois dès 2007, aux premiers frémissements de cette tendance. Quelques années plus tard, celle-ci est devenue un mouvement de fond. Pionnier de celui-ci, Brian Chesky, le fondateur d'Airbnb, est convaincu qu'il signe la fin de l'ère de la propriété : « On va passer d'une économie physique, où l'on échange des biens et services, à une économie où l'important sera le partage d'expériences[10] », déclarait-il au forum de Davos, en janvier 2014. Plus besoin de posséder, il suffit de vivre. Et de payer.

Les désillusions de l’économie du partage

Mais au fil des années, les promesses fabuleuses des chantres de « l’économie du partage » ont fait beaucoup de déçus. Si ces services, très compétitifs, ont conquis un large public, le terme « partage » s’est révélé trompeur. Les utilisateurs ont compris, peu à peu, que dans l’économie du partage, une part de choix était toujours réservée à la plateforme de mise en relation : 12 % du tarif chez Airbnb (3 % acquittés par l’hôte et 6 à 12 % par le voyageur), et 20 à 25 % chez Uber (selon les pays). Au fil des années, les conditions se sont dégradées pour les chauffeurs Uber (le prix minimal de la course a diminué, la commission prise par Uber a augmenté), si bien que le groupe californien a reçu des plaintes, un peu partout dans le monde, de la part de conducteurs mécontents qui réclamaient l’obtention du statut de salariés (aux États-Unis, au Royaume-Uni et en France notamment). En installant respectivement leurs sièges sociaux européens en Irlande et aux Pays-Bas, des pays à faible imposition sur les sociétés, Airbnb et Uber se sont aussi illustrés par leur virtuosité fiscale, qui leur a permis de payer un très faible impôt sur les bénéfices en France[*3]. Pour le partage, le Trésor public français repassera. La *sharing economy* a donc perdu de son lustre, au point que les professeurs de marketing Giana M. Eckhardt (Royal Holloway University of London) et Fleura Bardhi (Cass Business School, City University of London) proposaient, dans un article publié début 2015 dans la *Harvard Business Review*, de la rebaptiser : « Quand le “partage” a lieu par le biais d’un tiers – quand une entreprise fait office d’intermédiaire entre des consommateurs qui ne se connaissent pas – il ne s’agit plus du tout de partage. Il s’agit plutôt de consommateurs qui paient pour accéder aux biens ou services de quelqu’un d’autre pour une certaine période. […] C’est une économie de l’accès bien plus qu’une économie du partage[11] », tranchent-elles. Le terme paraît plus juste.

Uber en pair à pair

Une vraie économie du partage est toutefois possible, à condition de faire disparaître l’intermédiaire central (Uber, Airbnb ou autre) et de le remplacer par un logiciel pair à pair, connecté sur une blockchain (exactement comme OpenBazaar vis-à-vis d’Amazon). Plusieurs développeurs israéliens ont tenté de le prouver en créant LaZooz, en octobre 2013 : une application décentralisée de covoiturage et transport à la demande, sans intermédiaire, entièrement sous le contrôle de la communauté des participants. Son principe est simple : en conduisant d’autres usagers, un membre gagne des points (« zooz », la cryptomonnaie de la blockchain LaZooz), qu’il peut dépenser plus tard pour s’offrir un trajet dans la voiture conduite par un autre membre. « Pendant mon post-doctorat, j’ai eu l’idée de créer une application covoiturage en temps réel, la Zooz », raconte l’un des cofondateurs, Matan Field, qui a aujourd’hui quitté l’aventure. « Nous réfléchissions à une manière de rendre le projet plus coopératif, quand nous avons découvert la blockchain et son incroyable potentiel. LaZooz est vite devenu un projet blockchain », poursuit-il. Malheureusement, trois ans plus tard, cette initiative d’avant-garde, qui a fait beaucoup parler d’elle dans la presse, n’a toujours pas été concrétisée : l’application est bien disponible

en téléchargement, mais aucune voiture ne circule encore sous la bannière de LaZooz. « LaZooz existe toujours, mais personne ne travaille activement dessus à ma connaissance », précise Matan Field.

Uber peut-il alors dormir tranquille ? Pas tout à fait. Car aux États-Unis, un nouveau rival est né : Arcade City. Fondée à Portsmouth (New Hampshire) par un ancien chauffeur Uber, Christopher David, cette application de transport à la demande promet d'utiliser la blockchain Ethereum pour offrir un service comparable à celui d'Uber, mais plus avantageux pour les clients et les conducteurs. « Quand je conduisais pour Uber, a confié Christopher David au site Inverse.com, et que je pestais contre certaines règles de l'appli […], j'ai commencé à rêver d'une version décentralisée d'Uber sur une blockchain. » Début 2016, cette vision se concrétise sous la forme de l'application Arcade City. Sur celle-ci, dans sa dernière version présentée en septembre 2016, les passagers peuvent fixer le prix de la course. Ils publient une annonce pour le trajet qu'ils souhaitent effectuer, assortie d'une proposition de tarif (évalué par l'application) en ARC : des jetons Arcade City, que l'on peut acquérir avec des Ethers, la devise d'Ethereum. Le chauffeur a la liberté d'accepter ou non ce trajet pour la somme annoncée (tandis que sur Uber, plusieurs refus consécutifs peuvent valoir une suspension temporaire du compte). En acceptant, il signe le *smart contract* proposé par le client sur la blockchain Ethereum. Une fois à destination, la somme (en ARC) est reversée au chauffeur. Sur la transaction, l'application prélève une commission (le système n'est donc pas tout à fait désintermédié), mais celle-ci est nettement plus faible que celle d'Uber et de ses concurrents (10 % au lieu de 20 à 25 % chez le géant californien). Selon un communiqué d'Arcade City, la version bêta (test) de l'application, disponible en téléchargement entre mars et mi-avril 2016, aurait été utilisée par plus de 3 000 chauffeurs, dans 27 états américains et en Australie[12]. Elle a été retirée de l'App Store mi-avril, dans l'attente d'une version finalisée. Arcade City, surnommée le « Uber killer », a énormément fait parler d'elle dans la presse. Avec sa promesse aguichante « d'uberiser Uber », elle est l'un des projets blockchain les plus médiatisés. Mais sa nouvelle version, dévoilée le 1er septembre 2016, a déçu : elle ne permet pas d'être utilisée tant qu'un certain nombre de chauffeurs et de clients ne sont pas enregistrés dans le système (ce qui fait qu'aux derniers jours de décembre 2016, personne ne roulait avec Arcade City). Cette déconvenue a semé le doute sur le sérieux de l'entreprise. Arcade City a levé des fonds en vendant ses jetons ARC (environ 600 000 dollars au 21 novembre 2016), mais ces derniers ne peuvent pas être dépensés pour le moment. Pourront-ils l'être un jour ? Certains en doutent. D'autres critiquent la fausse décentralisation promise par Arcade City : l'application, qui prélève 10 % sur les transactions, reste en effet un intermédiaire central dans l'échange, même si celui-ci est réglé en cryptomonnaie. Et si elle promet, à terme, d'être entièrement détenue par ses utilisateurs, une fois de plus, il ne s'agit que d'une promesse. Enfin, la personnalité et le management du fondateur ont été remis en question par d'anciens collègues auprès de qui il s'était endetté et qui l'ont poursuivi en justice[13] – au point que Christopher David (dont le vrai nom est Christopher Pille) a dû se justifier sur le compte Facebook d'Arcade City : « J'ai mené des projets de création d'entreprise qui ont échoué par le passé, je dois également beaucoup d'argent à titre personnel. Je suis très mauvais pour gérer mes propres finances[14] », a-t-il ainsi avoué, avant d'assurer que le cas d'Arcade City est tout à fait différent : « J'ai fait beaucoup d'erreurs et j'ai appris de celles-ci. Ainsi va la vie d'un entrepreneur :

vous échouez et échouez et échouez, jusqu'à réussir. Arcade City est une réussite jusqu'à maintenant et continuera à l'être », assurait-il alors, le 2 avril 2016. Quelques mois plus tard, en novembre 2016, pour mettre fin aux spéculations sur sa capacité à diriger le projet, Christopher David a finalement démissionné de son mandat de patron de l'entreprise (plus précisément de maire du conseil des membres, dans le jargon de la start-up).

Quelle conclusion tirer de cette aventure initialement prometteuse et probablement mal partie ? D'abord, qu'Uber, Lyft, Blablacar, Heetch et autres grands intermédiaires du transport à la demande peuvent pour l'instant rester sereins face à ces concurrents guère menaçants. Comme dans tous les services d'accès, la taille du réseau (de chauffeurs, de clients, de villes desservies) est un avantage décisif, qui étouffe la concurrence. « Pour concurrencer vraiment Uber, vous devez recréer le même service qu'eux en termes d'offre et demande, et en plus créer la brique technologique sur la blockchain[15] », commente, sceptique, François Dorléans, le cofondateur de Stratumn, observateur attentif des projets du secteur. Mais après tout, Uber a bien réussi à constituer cette offre, dans un marché qui apparaissait verrouillé. Une autre conclusion s'impose : l'enthousiasme qu'ont suscité des projets pourtant très peu aboutis comme Arcade City ou LaZooz prouve qu'il y a une attente très forte, chez les consommateurs et les conducteurs, d'un service plus équitable. D'autres entrepreneurs sauront peut-être relever le défi avec plus d'acharnement, de sérieux et *in fine*, de succès.

Un verrou défie Airbnb

Comme Uber, Airbnb est aussi la cible de certaines start-up, qui rêvent de remplacer la plateforme et ses 12 % de commission par des systèmes mêlant objets connectés et logiciels actionnant des *smart contracts* sur une blockchain. Et s'il suffisait d'un verrou intelligent pour concurrencer le géant californien ? Cette idée un peu folle est le concept initial de Slock.it, une PME de cinq salariés basée en Allemagne, fondée par les Allemands Simon et Christoph Jentzsch et le développeur français Stephan Tual[*4]. « En code informatique, un verrou, c'est zéro ou un, ouvert ou fermé. En partenariat avec des sociétés de verrous connectés (comme Lock 8), on intègre à ces serrures notre technologie, qui permet aux gens de louer à distance leur appartement ou leur bureau », résume Stephan Tual. Un *smart contract*, inscrit dans la blockchain Ethereum, garantit l'ouverture de la porte au client, sa fermeture à son départ, et le versement de la somme due au loueur. Plus besoin d'Airbnb pour sécuriser la transaction, dont la bonne exécution est garantie par le *smart contract*. « Avec ce verrou électrique, je n'ai plus besoin d'être présent pour donner les clés, je récupère 100 % de l'argent de la location et j'ai le contrôle complet de ma plateforme », promet Stephan Tual. Bien sûr, un verrou électrique ne suffira pas à faire tomber le colosse de San Francisco. Il faudrait aussi reproduire le catalogue de biens en ligne. Pour cela, deux solutions : soit la communauté des utilisateurs pourrait elle-même créer, alimenter et faire vivre ce catalogue, soit une société pourrait s'en charger, en contrepartie d'une petite commission sur les locations.

Si le projet voit le jour, des problèmes juridiques ne manqueront pas de se poser, souligne l'avocat Simon Polrot, sur son blog Ethereum France : « Au-delà de la validité et de l'exécution des contrats, la problématique de la responsabilité sera également déterminante. Imaginons qu'une personne utilisant un appartement loué de façon décentralisée démarre un incendie dans cet appartement, qui fait une victime dans l'immeuble. Qui est responsable ? Qui paye l'indemnité et rembourse les dégâts ? Le propriétaire ? Il n'avait pas le contrôle de l'appartement quand l'incendie s'est produit. Le locataire ? Mais il n'a pas formellement signé de contrat de location et a juste obtenu l'accès à l'ouverture de la porte. Et si le locataire n'a pas donné sa véritable identité ? Qui contrôle ? Nul doute que les assurances qui seront appelées en garantie dans ces sinistres vont s'assurer d'épuiser tous les recours juridiques dont elles disposent pour éviter de payer quoi que ce soit… Des problèmes se poseront également au niveau réglementaire (*quid* des obligations légales qui pèsent sur les bailleurs, des règles KYC, etc.), fiscal (qui paye des impôts et comment ? quelle est la nature des revenus ? quel État peut taxer ?) voire pénal[16]. » Si l'on ajoute à ces soucis juridiques les défis techniques (bâtir un système fiable, sécurisé) et commerciaux (constituer un réseau d'utilisateurs suffisamment grand pour que le système de location soit intéressant), on voit que la route est encore longue avant que Slock.it ne puisse rivaliser vraiment avec Airbnb. Même si cet objectif immensément ambitieux n'est jamais atteint, le concept de verrous connectés à la blockchain de Slock.it trouvera sans doute son public à court terme, parmi les professionnels dans un premier temps – pourquoi pas des entreprises sous-louant à distance un bureau, une salle de réunion ou encore un hangar ? « Nous espérons pouvoir mettre des produits sur les étagères dès 2017 », précise Stephan Tual.

Cloud distribué : le nuage éparpillé

Comme le e-commerce, les réseaux sociaux et l'économie du partage, les services de cloud[*5] pourraient, eux aussi, être bientôt réinventés par la technologie blockchain. Ce marché colossal, en pleine croissance, suscite la convoitise : en septembre 2016, le cabinet d'études américain Forrester Research estimait qu'il devrait gonfler de 22 % par an entre 2015 et 2020 pour atteindre alors la bagatelle de 236 milliards de dollars[17]. Or les géants qui se partagent ce formidable gâteau (Microsoft, Amazon, Google) offrent des prestations qui, sous bien des aspects, prêtent le flanc à la critique : la centralisation, dans leurs serveurs, des données de centaines de millions d'utilisateurs les rend vulnérables au hacking et à la surveillance des agences américaines, comme la NSA. De plus, ces données sont utilisées pour vendre de la publicité ciblée aux annonceurs, d'une manière qui finit par agacer bien des internautes.

Décentraliser le nuage

Pour éviter ces écueils, plusieurs start-up proposent donc des solutions de « cloud distribué » : les données ne sont alors pas centralisées sur les serveurs de la société, mais hébergées dans les multiples ordinateurs des participants. C'est le principe de Storj, une start-up fondée en 2015, basée à Atlanta (États-Unis), qui offre à ses usagers une plateforme de cloud impossible à censurer, à surveiller ou à éteindre. Storj se définit comme « la première solution décentralisée et intégralement cryptée de stockage dans le cloud, utilisant la blockchain et la cryptographie pour sécuriser les fichiers ».

Le concept est ingénieux : les fichiers sont cryptés, puis découpés en multiples morceaux et stockés séparément dans un réseau décentralisé constitué d'ordinateurs, un peu partout dans le monde, dont les membres acceptent de louer l'espace libre de leur disque dur contre un paiement dans la cryptomonnaie de Storj (SJCX). Grâce à la fragmentation du fichier, personne n'en a de copie complète, même sous une forme cryptée. Seul le possesseur du fichier a la possibilité de le reconstituer pour le lire. Avec cette solution, Storj affirme être plus compétitif que les services traditionnels de cloud : plus rapide (car de multiples machines hébergent le fichier), plus sécurisé (car les fichiers sont cryptés et découpés) et potentiellement moins cher (car il n'y a pas besoin de bâtir de data centers pour toutes ces données, qui profitent de la puissance du réseau d'ordinateurs membres). Le tarif affiché, 0,015 dollar par GB (gigaoctet) par mois, est en réalité pour l'instant comparable à celui de Google Cloud Platform (0,007 à 0,026 par GB par mois, selon les prestations). La solution avait déjà séduit, à l'été 2015, 3 800 utilisateurs qui ont stocké plus de 2 TB (teraoctets) – l'équivalent de 4,4 millions de fichiers Word comme celui sur lequel ce brillant essai a été écrit.

D'autres start-up, comme Sia, dont le projet a germé lors d'une hackathon organisé au MIT (Massachusetts Institute of Technology) en 2013, affichent la même volonté : créer un cloud décentralisé sur la blockchain, qui mettrait à profit l'espace de stockage inutilisé d'un réseau d'ordinateur dispersé aux quatre coins de la planète. Chez Sia, les transactions sont réglées dans la cryptomonnaie de la blockchain dédiée à la gestion de cet hébergement distribué, le Siacoin. Le système fonctionne et est même très compétitif : en janvier 2016, le prix de stockage affiché était d'environ 2,25 dollars par TB et par mois, soit 0,001 dollar par GB et par mois. Au 21 novembre 2016, près de 445 000 fichiers y étaient hébergés. Face à ces nouveaux venus encore minuscules mais potentiellement menaçants, les géants du cloud ne veulent pas se laisser déborder. Microsoft s'est ainsi allié à la start-up brooklynienne Consensys, pour mettre à disposition de ses clients (entreprises et développeurs), dans son cloud Azure, des outils permettant le développement d'applications décentralisées sur Ethereum (EtherCamp et BlockApps). Mais il s'agit encore finalement d'un service de cloud traditionnel centralisé, qui donne accès à distance à un environnement destiné aux développeurs Ethereum, et non d'un service de cloud décentralisé.

Des sites Web incensurables

Dans un genre différent, ZeroNet, projet imaginé fin 2014 par un développeur hongrois, Tamas Kocsis, 32 ans, permet, lui, d'héberger de manière décentralisée, non pas des fichiers ou des logiciels,

mais des sites Internet, au lieu de faire appel à un serveur. ZeroNet utilise pour cela à la fois la blockchain Bitcoin et BitTorrent, un protocole qui permet le transfert de fichiers en pair à pair, afin de permettre aux sites qui s'y inscrivent de devenir incensurables[*6]. Début septembre 2016, ZeroNet comptait seulement un millier d'utilisateurs environ, venant de Chine, d'Europe, d'Amérique du Nord, de Malaisie, d'Indonésie ou encore d'Australie. L'initiative reste donc marginale à ce jour. Mais sa promesse de permettre la création de sites incensurables présente une réelle plus-value, pour le meilleur – dans les pays qui exercent une censure forte sur le Web – ou pour le pire (en permettant potentiellement aussi la résilience de sites criminels ou terroristes).

Interrogé sur les risques de dérives de ZeroNet, le fondateur s'est voulu rassurant : « Je crois que ZeroNet peut être intéressant pour n'importe quelle personne souhaitant exercer sa liberté d'expression[18] », a affirmé Tamas Kocsis au journal britannique *International Business Times*. « Il serait possible de créer des sites illégaux sur ZeroNet, mais je ne crois pas que ce soit l'outil idéal pour cela, car sur ZeroNet, chaque visiteur est aussi l'hôte du site qu'il visite, et je pense que la plupart des gens ne veulent pas héberger ce type de contenu », a-t-il expliqué, n'admettant avoir vu qu'un seul site hébergé sur ZeroNet où des services de hacking étaient proposés. Au printemps 2016, ZeroNet s'était toutefois fait remarquer en affichant, parmi ses tout premiers sites hébergés, « Play », un service de partage de liens de téléchargement pair-à-pair illégaux, *a priori* impossible à fermer, contrairement aux précédentes grandes plateformes de téléchargement illégal comme The Pirate Bay, dont les sites ont été saisis par la justice suédoise le 19 mai 2015. Preuve que l'esprit cryptoanarchiste des origines du Bitcoin n'a pas totalement disparu.

Musique, culture et médias : rendre le pouvoir à ceux qui créent

Qu'y a-t-il de commun entre un musicien, un photographe et un journaliste ? Tous les trois créent un contenu original (un morceau, une photo, un article), le cèdent à un grand groupe (majors du disque ou des médias, agence), sont de moins en moins bien payés pour leur œuvre, que le grand groupe en question arrive de plus en plus difficilement à vendre à des clients, qui ne veulent plus payer pour ce genre de produits, convaincus qu'ils peuvent les trouver gratuitement. Si bien que tous, musiciens, photographes et journalistes, regrettent l'époque dorée d'avant Internet, dont les anciens leur rebattent les oreilles. Dans cette histoire, la chute n'est pas drôle : elle est en revanche brutale, et jusqu'à maintenant irréversible.

Alors qu'Internet a démultiplié comme jamais l'audience potentielle des artistes, des journalistes et de tous ceux que l'on peut regrouper sous l'étiquette, assez peu poétique mais claire, de « producteurs de contenus », le numérique a aussi plongé leurs secteurs respectifs dans des crises profondes, qui semblent, du point de vue des premiers concernés, interminables. Certes, dans la musique, après l'effondrement total des ventes de disques, de nouveaux *business models* ont fini par être trouvés avec le streaming, la vente à l'unité (Itunes) et surtout le retour à la scène, principale source de revenus des musiciens. Mais dans ce nouvel équilibre, les artistes ont beaucoup perdu au change : sur les sites de streaming, « les ayants droit touchent en moyenne 0,0001 euro par écoute gratuite (financée par la publicité) et entre 0,002 et 0,004 euro en flux payant, financé par les abonnements[19] », précisait un article du *Monde* publié en juin 2015. À ce rythme, il faut un million d'écoutes pour gagner entre 1 000 et 4 000 euros. Autant dire qu'il faut être sacrément bon pour s'assurer un smic mensuel en diffusant sa musique sur Deezer, Spotify ou Apple Music. « *Get rich or die tryin'*[*7] », chantait le rappeur 50 Cent. Lui ne l'est certainement pas devenu grâce au streaming. La vente d'une chanson en téléchargement légal est un peu plus rémunératrice, mais l'artiste a quand même perdu au change : selon une étude de l'Adami datée de 2013, sur un album vendu en version numérique, il touche 5,1 % du prix en moyenne, contre 6,4 % en version physique (CD ou vinyle – entre 1 et 50 000 exemplaires)[20]. Dans la presse, le constat n'est guère plus reluisant. En France, la quasi-totalité des groupes de presse, incapables de monétiser convenablement les articles sur

Internet, perdent de l'argent. Les plans de départ volontaires se multiplient (en 2016, à *L'Obs*, *L'Express*, *Libération*, au *JDD*, à *Paris Match*, *Elle*…). Le nombre de journalistes en activité, qui a chuté de 4 % entre 2009 et 2015, va continuer à décroître. À l'étranger, les grands titres ne s'en sortent guère mieux : toujours en 2016, *The Guardian*, quotidien de référence britannique, a lancé un plan d'économie, le *New York Times* a ouvert un guichet de départs volontaires, même le *Wall Street Journal*, qui vise pourtant une cible privilégiée, a enchaîné en novembre son deuxième plan de licenciements. Rien ne va plus !

Heureusement, une lueur d'espoir est peut-être en train de surgir dans ce paysage sinistré. De même que la musique, avant la presse, avait été la première industrie bouleversée par le numérique dès la fin des années 1990 (et aussi la première à trouver une manière de s'y adapter), c'est encore une fois dans le secteur musical que naissent des solutions qui pourraient peut-être, dans un deuxième temps, inspirer l'industrie des médias. En Israël, aux États-Unis et au Royaume-Uni, plusieurs start-up inventent ainsi de nouvelles manières de gérer automatiquement les revenus des ayants droit (auteurs, compositeurs, interprètes), voire d'assurer le financement participatif de leurs créations grâce à des *smart contracts* inscrits sur une blockchain. Avec une idée en tête : replacer l'auteur au centre et lui rendre une part plus équitable du gâteau.

La musique à l'avant-garde

Le 10 décembre 2014, le jeune musicien et investisseur américain D. A. Wallach, chanteur pop du groupe Chester French et diplômé d'Harvard, publiait sur le site Backchannel un article appelé à faire sensation dans le secteur de la blockchain et dans l'industrie musicale. Dans cette longue analyse intitulée « Le Bitcoin pour les rockstars. Comment la cryptomonnaie peut révolutionner l'industrie de la musique[21] », il suggérait de faire appel à une technique à l'époque tout à fait inattendue pour gérer l'épineuse question des droits des artistes. « Le Bitcoin offre une solution potentiellement fascinante au problème incroyablement ennuyeux auquel l'industrie musicale fait face, écrivait-il. Ce problème, c'est simplement qu'il n'existe aucune base de données centralisée pour conserver les informations sur la musique. Plus précisément, concernant un morceau, deux sortes d'informations sont particulièrement importantes : qui l'a créé et qui en possède les droits ? Actuellement, ces informations sont excessivement difficiles à retrouver, au plus grand détriment des artistes, des services de musique et des consommateurs. » Comment améliorer la situation ? « Des cryptomonnaies décentralisées, *open source* et mondiales comme le Bitcoin et Ripple […] offrent un modèle pour mettre fin à ce maudit *statu quo*. En utilisant l'avancée technologique apportée par ces réseaux, nous pouvons, pour la première fois dans l'histoire de l'humanité, organiser les données musicales d'une manière sensée et, plus important encore, réinventer la façon dont artistes et ayants droit sont rémunérés », promettait D. A. Wallach. Le jeune musicien businessman précisait même son idée : dans une blockchain des droits d'auteur musicaux, chaque chanson, chaque ayant droit (auteur, compositeur, interprète, héritier, maison de disques, producteur, etc.) et chaque personne voulant acquérir ou diffuser un titre (site de streaming, YouTube,

radio…) seraient identifiés par une adresse publique. La répartition instantanée des sommes à verser à chacun serait assurée par des *smart contracts* se répondant les uns aux autres, et garantissant à chaque partie son dû, immédiat, tout en permettant à tous d'observer, dans ce système transparent, l'activité économique réelle générée par la création.

L'expérience Ujo remet l'artiste au centre

Cette vision pionnière a, depuis, inspiré différents projets, dont le tout premier est l'expérience « Ujo », imaginée par le musicien britannique Phil Barry et testée avec la chanteuse anglaise Imogen Heap. Quand paraît l'article de D. A. Wallach, Phil Barry est en pleine réflexion sur la manière dont l'industrie musicale pourrait être réinventée de façon plus avantageuse pour ceux qui créent. « J'ai été un artiste pendant presque dix ans, sous le nom de Mr Fogg. J'ai fait des tournées, j'ai joué sur les scènes de grands festivals, je suis passé à la télé… J'ai aussi dirigé un label indépendant pendant cinq ans. Je me suis rendu compte qu'il était très difficile de faire de la musique un business qui marche, j'étais très frustré de ne pas réussir à avoir un minimum d'impact sur la structure de l'industrie musicale. Je me sentais impuissant et j'avais seulement le vague sentiment de vouloir améliorer l'état du secteur de la musique, qui n'avait pas su trouver de nouvelles opportunités depuis l'invention du mp3[22] », confie-t-il. Le jeune homme se plonge donc dans les livres, retourne sur les bancs de l'université le temps d'un MBA à Oxford et commence à développer des idées sur l'innovation numérique dans les modèles économiques de la musique. En 2014, il travaille comme consultant pour Thom Yorke, chanteur de Radiohead, sur un projet assez révolutionnaire : la sortie du deuxième album solo du chanteur, *Tomorrow's Modern Boxes*, en téléchargement sur la plateforme en pair à pair BitTorrent (pour la modique somme de 6 dollars). L'objectif de cette première expérience était déjà, selon Thom Yorke lui-même, de « permettre à ceux qui créent de la musique, des vidéos ou toute autre forme de contenu numérique de le vendre eux-mêmes, en s'affranchissant des intermédiaires autoproclamés[23] ».

C'est dans ce contexte de révolte des artistes contre les règles établies par l'industrie musicale que Phil Barry, à l'affût des nouvelles idées pour s'émanciper de la tutelle des maisons de disques, plateformes de streaming et sites de téléchargements légaux, découvre l'article de D. A. Wallach. « J'ai lu cet article et j'ai immédiatement compris le grand potentiel de la blockchain pour la gestion des droits. Depuis longtemps, j'étais embêté par la division des droits musicaux en deux catégories : droits d'auteur et droits voisins [des artistes-interprètes, des producteurs, des chaînes de télé et des stations de radio]. J'ai vu dans la blockchain une manière de cacher la complexité de ces différents types de droits dans une base de données unifiée liée à une infrastructure de *smart contract* », raconte-t-il. C'est ainsi que naît Ujo. « J'ai contacté l'auteur, D. A. Wallach, mais il n'avait pas envie de se lancer dans cette aventure. J'ai rencontré quelques personnes, dont des développeurs chez Ethereum, qui avaient été intéressées par son article, et nous avons commencé à construire Ujo en mai 2015 », précise-t-il. « Nous avons pris une chanson de l'artiste britannique Imogen Heap, *Tiny Human*, et avons essayé d'imaginer une utilisation concrète de la blockchain pour l'infrastructure de royalties. L'objectif était de prouver que cela pouvait

être un mécanisme efficace pour gérer les informations relatives aux droits, que nous pouvions utiliser des *smart contracts* pour faciliter la vente de licence [pour une utilisation commerciale la chanson dans une publicité par exemple] ou le téléchargement direct aux auditeurs, en pair à pair sans intermédiaires, et que nous pouvions dans la foulée redistribuer instantanément les royalties aux ayants droit (ce qui peut prendre quatre ans aujourd'hui) », développe Phil Barry.

Le site pionnier, alpha.ujomusic.com, a été mis en ligne le 2 octobre 2015. N'importe qui, professionnel ou particulier, peut y acheter la chanson. Elle est disponible soit en téléchargement simple pour 0,6 dollar, soit en fichier « stem[*8] » pour un usage professionnel, de remix par exemple, pour 45 dollars, soit en streaming pour 0,006 dollar l'écoute, soit pour des utilisations commerciales, comme une publicité (le prix est alors à discuter). Dans chaque cas, la répartition des droits est précisée. Par exemple, sur un téléchargement à 0,60 dollar, Imogen Heap touche 91,25 % des droits, et ses 7 instrumentistes, 1,25 %. Quand la transaction a lieu (en Ethers), elle est inscrite dans la blockchain Ethereum, où des *smart contracts* distribuent la somme selon les conditions inscrites dans le code. Avec un tel système, l'artiste – Imogen Heap dans ce cas – est triplement gagnante. D'abord, c'est elle qui vend ses productions et non plus une maison de disques à qui elle aurait cédé ses droits. Il n'y a plus, ou moins, d'intermédiaires et sa part du gâteau est plus grande. Ensuite, l'artiste est payée tout de suite. Enfin, elle bénéficie d'une plus grande transparence : elle reçoit automatiquement ce qui lui est dû selon les conditions écrites dans le *smart contract*. « À l'avenir, quand quelqu'un achètera ou diffusera un titre de musique, il n'y aura plus besoin d'un intermédiaire centralisé. Les fans pourront immédiatement payer l'artiste[24] », a déclaré Imogen Heap au magazine *Quartz*, en février dernier. Même pour les grandes entreprises du secteur de la musique, le système peut être avantageux car il est efficace : grâce à l'automatisation des royalties, « certains estiment que la blockchain peut diminuer les frais de personnel de 25 % », note Phil Barry. La gestion transparente et automatisée des droits sur la blockchain permet également d'éviter les conflits entre les ayants droit : une seule base de données, partagée entre eux, fait foi.

De multiples projets parallèles

Cette expérience éphémère a depuis donné naissance à plusieurs projets parallèles. Imogen Heap elle-même s'est lancée dans Mycelia, une fondation qui vise à développer un « commerce équitable de la musique » au profit des artistes, en s'inspirant des registres blockchain. Pour l'instant, Mycelia est plutôt un lieu de réflexion qu'un service. « Mycelia veut observer l'architecture de ce qui existe déjà, explorer de nouvelles technologies comme la blockchain et élaborer le meilleur scénario pour les musiciens[25] », résume l'artiste dans un article du site britannique Tech City News. Le projet initial, Ujo (devenu Ujo Music), est poursuivi par la start-up new-yorkaise Consensys, qui développe une plateforme, sur Ethereum, pour reproduire avec n'importe quel titre le mécanisme utilisé pour le titre *Tiny Human*. « Ujo Music permettra aux artistes ou aux ayants droit d'enregistrer des contenus sur la blockchain et de définir des politiques d'utilisation, afin que le consommateur puisse acquérir une licence d'utilisation de ce

contenu aux conditions fixées, pour un usage privé, public, ou pour mettre le titre en bande-son d'une vidéo par exemple. La licence pourra être acquise immédiatement et l'argent sera versé en temps réel à l'artiste[26] », résume le fondateur de Consensys, Joseph Lubin. Une version bêta de l'application est annoncée au printemps 2017.

De son côté, Phil Barry a quitté Ujo et ouvert une start-up sur le même concept : Blokur, qui vise à étendre le concept d'Ujo, limité à une chanson. Pour réussir, il mise sur la collaboration avec les grands acteurs du secteur plutôt que sur la confrontation. L'entrepreneur prépare des projets avec deux des trois plus grands services de streaming au monde et une grande maison de disques. Son objectif, précise-t-il, n'est pas de se substituer à Spotify ou Itunes, mais de remplacer l'infrastructure qui existe derrière leur service. *Quid* alors de l'ambition initiale de supprimer les intermédiaires entre artistes et consommateurs ? « Le nombre d'intermédiaires entre les deux bouts de la chaîne est très important. Il y a beaucoup d'inefficacité là-dedans. Si nous pouvons automatiser les choses, cela conduira à une certaine désintermédiation. Nous n'éliminerons pas les producteurs et les éditeurs de musique, mais les artistes devraient avoir le choix de travailler ou non avec eux », justifie-t-il. Le jeune entrepreneur sait qu'il lui reste du chemin à parcourir : « Nous en avons au moins encore pour un an, car la technologie blockchain doit progresser sur bien des points, comme le respect de la confidentialité et la "mise à l'échelle[*9]" », admet-il.

Simplifier la gestion des droits

Pour aller plus vite, Blokur a participé à la fondation de l'Open Music Initiative (OMI), un projet sectoriel lancé en juin 2016 par l'institut d'entrepreneuriat créatif de Berklee (célèbre école musicale new-yorkaise). En partenariat avec les plus grands noms de l'industrie (Universal Music Group, Sony Music Entertainment, Warner Music Group, BMG, Spotify, YouTube, Pandora, SoundCloud, Netflix mais aussi la Sacem), OMI, une organisation à but non lucratif, tente de créer un protocole *open source* pour uniformiser l'identification des ayants droit et créateurs de musique, et de définir des spécifications techniques qui permettront l'interopérabilité des plateformes de gestion de droits des différents acteurs. En des termes moins abscons, OMI veut s'assurer que la révolution blockchain permettra vraiment de garantir aux artistes et ayants droit le versement des revenus qui leur sont dus et qui sont, depuis trop longtemps, perdus dans la nature. Outre Blokur, plusieurs start-up blockchain font partie de l'aventure, dont la PME israélienne Revelator, fondée au printemps 2015 par Bruno Guez, un producteur franco-américain établi à Tel Aviv. Revelator ne cherche pas à supprimer tous les intermédiaires pour mettre artistes et auditeurs en relation directe, mais plutôt à simplifier la gestion des droits pour les professionnels de la musique. Avec cette visée moins glamour, mais plus réaliste et rentable, l'entreprise a réussi à lever pas moins de 2,5 millions de dollars de fonds fin août 2016. Si le service offert par Revelator intéresse, c'est qu'à l'ère numérique, la répartition des droits est devenue un sac de nœuds quasi ingérable par ceux qui sont pourtant dans l'obligation contractuelle de le faire (sociétés de droits d'auteur, distributeurs, majors de la musique, etc.). « L'année dernière, l'équivalent britannique de la

Sacem (société de gestion des droits d'auteurs de la musique) a dû gérer 2 400 milliards de transactions. C'est exponentiel. Chaque année, ça double ou ça triple. Et je ne cite qu'une seule société de droits d'auteurs, alors qu'il y en a des centaines dans le monde. Avec quelque 150 millions de chansons dans les catalogues, il faut les aider à gérer cette explosion de données numériques[27] », affirme Bruno Guez. Avec la blockchain, l'automatisation de la gestion de ces milliards de transactions, souvent minuscules, devient possible : « Elle permet d'enregistrer un actif et les droits qui y sont liés, et de les associer à un *smart contract*, qui est exécuté en fonction des transactions. Ce *smart contract* automatise la distribution des droits et royalties en fonction des règles établies sur le bien (qui peut être une chanson ou autre chose) », indique l'entrepreneur. Revelator a bâti sa propre blockchain privée (pour préserver la confidentialité des transactions) et offre à ses clients un service accessible sur son site. Artistes, managers et labels peuvent charger un morceau, dont ils ont les droits, dans le cloud de Revelator et sélectionner des diffuseurs (Spotify, Itunes, SoundCloud, Deezer, Amazon…). Revelator s'occupe ensuite automatiquement de reverser les sommes dues aux intéressés, en fonction du nombre d'écoutes et des conditions contractuelles, transcrites dans des *smart contracts*. Le service est facturé 10 dollars par mois pour un artiste, 60 pour un manager et 100 pour un label.

Financer la création

Bruno Guez voit plus loin. Il envisage, dans un deuxième temps, d'étendre sa plateforme au financement de la création, financement auquel les fans seraient invités à participer : « La vitalité et la rapidité des transactions sur une blockchain peuvent permettre plus de liens directs entre consommateurs et artistes, par exemple pour laisser un fan avoir accès en premier à la musique de son chanteur préféré ou même acheter des parts dans un morceau », parie-t-il. « En 2017, j'aimerais développer un marché pour l'échange de droits intellectuels, le CAC 40 ou le Kickstarter[*10] de la musique. Tu as une appli mobile, tu achètes et tu vends des actions de musiques, pour aider les artistes à lever des fonds », précise Bruno Guez. À New York, la start-up Consensys travaille elle aussi à intégrer les fans dans le financement de la création. « Nous avons développé un outil de gouvernance appelé Board Room, qui peut être utilisé par exemple par un groupe de musique [ou tout autre type d'organisation]. Imaginons que vous ayez un groupe, décrit Joseph Lubin. Vous voulez des règles transparentes qui précisent qui possède quoi dans les morceaux que vous créez. Vous pouvez alors utiliser Board Room pour le définir, émettre des jetons [qui représentent le capital du groupe, réparti entre les membres] et éventuellement en vendre une partie pour lever des fonds, dans un système de financement participatif. Par exemple, vous vendez 20 % des recettes de la prochaine tournée afin d'intégrer les fans au business. En échange, vous les laissez choisir quels titres iront sur l'album, voire suggérer des changements sur des chansons. » Joseph Lubin est confiant : « Un tel système ouvre un vaste nouveau territoire pour les artistes. Nous avons discuté avec beaucoup d'entre eux, qui ont tous hâte d'essayer la plateforme. »

Si la blockchain arrive à gérer des processus aussi compliqués que le versement en continu de sommes, parfois minuscules, à des millions d'ayants droit dans la musique, alors pourquoi ne pourrait-elle pas être utilisée dans les autres secteurs de la création ? Cinéma, presse, télévision, édition, arts plastiques… Tout ce qui relève de la propriété intellectuelle pourrait potentiellement trouver un intérêt dans l'automatisation de la gestion des droits permise par des *smart contracts* sur la blockchain. Très peu de projets ont pour l'instant été annoncés dans ces secteurs. Mais ces derniers pourraient bien prendre rapidement le même chemin que la musique. Bruno Guez en a la ferme intention : « J'envisage qu'on s'attaque dans les prochains mois à la vidéo, puis à tout ce qui est broadcast [diffusion radio ou télé] » confie-t-il. Chez Consensys, l'ambition est la même : « Très bientôt nous commencerons Ujo film pour le cinéma et Ujo pour l'industrie de l'art », promettait Joseph Lubin à l'été 2016.

En France, l'intérêt de cette technologie n'a pas échappé au ministère de la Culture. Le Conseil supérieur de la propriété littéraire et artistique (CSPLA), organisme chargé de conseiller le ministre de la Culture sur les questions juridiques, a commandé un rapport d'étude, qui devrait être rendu au printemps 2017, sur l'impact potentiel des applications décentralisées sur la blockchain pour l'univers des biens culturels : « Il s'agira notamment d'évaluer ses apports pour la gestion des droits, l'accès aux œuvres ou encore l'optimisation des divers modes d'exploitation[28] », écrivait le président du CSPLA, Pierre-François Racine, dans la lettre de mission, publiée le 8 juillet, soulignant au passage son propre enthousiasme : « Ces applications apparaissent comme prometteuses en raison des simplifications, de la sécurité et des baisses de coût de transactions, notamment contractuelles, qu'elles pourraient apporter. »

Une chance à saisir pour la presse

De tous les secteurs culturels, celui qui résiste le moins bien aux bouleversements du numérique est la presse. Or la technologie blockchain, et en particulier le Bitcoin, pourrait résoudre le principal problème que rencontrent les groupes de médias depuis l'arrivée d'Internet : leur incapacité à vendre des articles en ligne d'une manière suffisamment massive et rentable pour compenser la disparition progressive des acheteurs de journaux imprimés. Après avoir poursuivi pendant toutes les années 2000 une désastreuse stratégie de mise en ligne gratuite de leurs articles, en misant tout sur des recettes publicitaires qui se sont avérées dérisoires, les grands groupes de presse ont fini par comprendre que leur seule chance de survivre était de faire payer leurs lecteurs sur Internet. Mais entre-temps, beaucoup d'internautes ont perdu l'habitude de payer pour s'informer. La tâche est donc difficile. Ces dernières années, des offres de *paywall* (des abonnements obligatoires après quelques articles consultés) ont fini par émerger. Petit à petit, ces abonnements rencontrent un succès grandissant, mais qui reste très insuffisant pour faire vivre les rédactions. En réalité, il manque une dimension importante à l'offre des journaux : pour lire en ligne un titre de qualité, il faut désormais s'abonner. La possibilité d'acheter occasionnellement le journal, comme on peut le faire au kiosque, a quasiment disparu car les groupes de

médias n'ont pas, jusqu'ici, réussi à développer la vente d'articles à l'unité. Certains la proposent (comme LeMonde.fr), mais à des prix ridiculement élevés : 2 euros l'article, soit le prix du journal entier en version imprimée… Qui n'aurait pas l'impression de se faire avoir dans ces conditions, alors même que le coût de la publication en ligne, pour le journal, est quasiment nul comparé à l'impression traditionnelle ? Ce tarif exorbitant a une explication : il est dû au coût tout aussi dissuasif du règlement de petites sommes (micropaiement), facturé par des intermédiaires du paiement (compagnies de cartes de crédit, Paypal, etc.). Or le Bitcoin et les autres cryptomonnaies permettent précisément de s'affranchir de ces acteurs, et ainsi de rendre possible, peu coûteux et instantané l'achat d'un article, en un ou deux clics, pour une somme modique.

Cette idée a été formulée dès janvier 2014 par l'investisseur Marc Andreessen, dans une tribune publiée dans le *New York Times* : « Les micropaiements n'ont jamais été possibles, malgré vingt années de tentatives infructueuses, parce qu'il n'est pas rentable de faire transiter des transactions de petites sommes (un dollar ou moins, voire quelques centimes ou fractions de centimes) à travers le système actuel de banques et cartes bancaires. […] Tout d'un coup, avec le Bitcoin, cela devient trivialement simple. Les Bitcoins ont la formidable propriété d'être divisibles à l'infini : actuellement, jusqu'à 8 décimales après la virgule, et plus encore à l'avenir. Vous pouvez donc indiquer une toute petite somme d'argent, comme un millième de centime, et l'envoyer à quiconque partout dans le monde gratuitement ou presque. Pensez donc à la monétisation du contenu, par exemple. Une des raisons pour lesquelles les groupes de médias et journaux ont des difficultés à faire payer leur contenu est qu'ils facturent soit tout – un abonnement global à tout le contenu –, soit rien – ce qui se traduit par ces affreuses bannières publicitaires un peu partout sur le Web. Soudain, avec le Bitcoin, apparaît une manière économiquement viable de faire payer de petites sommes d'argent par article, ou par rubrique, ou par heure, ou par vidéo, ou par accès aux archives, ou encore par alerte info[29]. » Deux ans plus tard, personne n'a encore saisi l'opportunité. Pourtant d'autres experts confirment le diagnostic de Marc Andreessen, comme les analystes de l'agence Moody's, qui, dans un rapport de juillet 2016, font le parallèle entre musique et médias : « Une blockchain de droits digitaux pour des produits de consommation, comme de la musique et des articles de presse, entre autres, permettrait, grâce des *smart contracts*, de garantir que les artistes ou les auteurs sont payés dès qu'un consommateur a lu un article ou écouté une chanson, proportionnellement aux conditions précisées dans le contrat. Étant donné les faibles coûts de transaction sur une blockchain, les micropaiements deviendraient économiquement viables, ce qui rendrait possible le paiement à l'usage, à chaque fois qu'un article est lu ou qu'une chanson est écoutée[30]. » Imaginons par exemple que LeMonde.fr facture la lecture d'un article 10 centimes d'euros, au lieu de 2 euros, avec un système de paiement extrêmement simple, sécurisé et rapide (en quelques clics). Le site reçoit environ 90 millions de visites par mois (Web et mobile)[31]. Si, en moyenne, un lecteur achetait un seul article lors d'une visite sur 5 sur le site ou l'application mobile, au prix de 10 centimes d'euros (ce qui paraît une hypothèse très conservatrice), LeMonde.fr générerait 1,8 million d'euros de chiffre d'affaires mensuel supplémentaire. Il est curieux que personne n'ait encore tenté l'aventure.

Coopératives de journalistes indépendants

Il y a toutefois une start-up blockchain qui s'est intéressée à la presse, mais avec une vision tout à fait différente, qui pourrait plaire aux journalistes, aux lecteurs, mais beaucoup moins aux groupes de médias : Backfeed, une entreprise créée par le physicien israélien Matan Field (cofondateur de LaZooz), Tal Serphos, ancien trader lui aussi israélien, et la chercheuse italienne Primavera De Filippi. Cette PME s'est spécialisée dans la conception de systèmes de gouvernance et de modèles économiques, régis sur la blockchain, pour des organisations décentralisées, afin de favoriser la collaboration massive des individus – et pourquoi pas des journalistes, suggère Matan Field : « Parmi nos cas d'usage, nous avons pensé aux médias décentralisés[32] », confirme-t-il. « Aujourd'hui, tout le monde est journaliste[*11], lance l'entrepreneur. Beaucoup de gens écrivent des contenus, parfois de mauvaise qualité mais aussi parfois très bons. Un triple problème se pose donc : d'abord, celui de la qualité et de la recherche. Il y a trop de contenus, et pour cette raison, le contenu ne vaut pas assez cher. On ne peut pas en vivre. Ensuite, il y a un problème pour le lecteur, qui, devant cette offre excessive, n'arrive pas trouver ce qu'il aimerait vraiment. Résultat, il n'est pas prêt à payer. Enfin, il y a un manque de tri, de sélection du contenu par les gens. La sélection (*curation*) est sous-évaluée. Les personnes qui cliquent sur like au bas d'un article sur un réseau social restent hors du circuit business. Avec une plateforme de contenu décentralisée, vous pouvez résoudre tous ces problèmes : vous générez de la valeur par le contenu que vous produisez et par votre participation à la sélection et la mise en avant [du contenu de qualité]. Les premiers lecteurs et les producteurs de contenu sont rémunérés de manière juste. C'est une situation dans laquelle tout le monde peut être gagnant », considère Matan Field.

Tout le monde… ou presque. Dans ce paysage où seuls existent ceux qui écrivent les articles, ceux qui les lisent et ceux qui les mettent en avant, que deviendraient les journaux ? Un souvenir d'une époque révolue. « Il n'y aurait plus de journaux, admet Matan Field, mais il y aurait bien des journalistes, qui pourraient coopérer, au sein de cercles que l'on pourrait appeler des journaux, même si ce serait plutôt des coopératives d'auteurs, travaillant ensemble avec des intérêts et une mentalité commune. Ce que l'on pourrait résumer par le concept de *crowdsourcing journalism*[*12] ».

Jouer, parier et deviner l'avenir

Secteur innovant s'il en est, toujours à l'affût d'une innovation technologique ou d'une manière d'échapper à des réglementations défavorables, le jeu au sens large – jeux vidéo, casino ou paris – a su s'emparer lui aussi des nouvelles possibilités ouvertes par les blockchains. Ouvrant même des perspectives insoupçonnées pour affiner notre vision de l'avenir…

Des jeux vidéo qui rapportent

Être payé pour jouer, combien de passionnés de jeux vidéo en rêveraient ? Plusieurs start-up l'ont compris et ont dévoilé, au second semestre 2016, des applications mobiles de jeu qui rémunèrent les joueurs en cryptomonnaie. Mise au point par une équipe franco-suisse, basée à Genève, l'application BitcoinBandit, commercialisée fin août 2016 sur les mobiles Android et iOS, promet de faire gagner tous ses utilisateurs. Après avoir enregistré dans l'application l'adresse publique de son portefeuille de Bitcoin, le joueur dirige un petit lapin et tente de récolter des pièces d'or, tout en évitant des obstacles. Chaque pièce rapporte un « Satoshi » (0,00000001 BTC) et les 10 premiers du tournoi raflent, en plus, une récompense plus substantielle en Bitcoins (dont le montant dépend du nombre de participants). « Nous sommes les premiers à installer une rémunération sur un jeu, c'est assez novateur[33] », confiait l'un des fondateurs, Guillaume Pedra, au quotidien *La Dépêche*. Pour financer cette distribution d'argent numérique, l'application reverse aux joueurs la moitié de ses revenus publicitaires. Dans l'univers des jeux mêlant stratégie et cartes (virtuelles) à collectionner, Spells of Genesis, la création de l'éditeur EverdreamSoft disponible sur le Web et sur mobile (Android et iOS en version bêta) depuis mi-septembre 2016, se vante, elle aussi, d'être le premier jeu basé sur la blockchain. Elle s'appuie sur une cryptomonnaie, les BitCrystals (raccrochés à la blockchain Bitcoin), qui servent à donner une valeur aux cartes que peuvent s'échanger les joueurs. Enfin, Beyond the Void, un jeu de stratégie multijoueurs, fonctionnant lui aussi avec des cartes à collectionner, devrait sortir en version bêta en février 2017 et

dans sa version commerciale en juin : les utilisateurs joueront gratuitement, mais pourront acheter des cartes spéciales avec des jetons, acquis en Ethers (les transactions seront donc enregistrées sur Ethereum).

Tous mes Bitcoins sur le rouge

Parallèlement à ces applications ludiques, les jeux d'argent (casinos et paris) ont, depuis quelques années déjà, vu débouler des applications blockchain, en particulier Bitcoin. Rarement légales, elles permettent à leurs créateurs et utilisateurs d'échapper aux réglementations de ces secteurs. Il existe d'innombrables casinos en ligne, dont Bitcoin Games, Bit777 ou encore 777coin. La firme Consensys a elle aussi, parmi ses nombreux projets, celui d'une application de poker sur Ethereum. Baptisée Etherpoker, elle permettrait aux joueurs de miser de manière simple, légale et sécurisée. « Beaucoup de gens veulent jouer au poker en ligne, mais la loi rend les choses difficiles. Souvent, le fait de jouer n'est pas interdit, mais les banques n'ont pas le droit d'accepter les flux financiers vers et depuis les sites de poker [*13]. Cela a entraîné la création de mécanismes compliqués pour permettre aux joueurs de miser de l'argent en ligne. Certaines plateformes ont fermé et ont volé l'argent des joueurs. Et c'est si compliqué de retirer son argent que personne ne le fait. Avec notre système, vous restez en contrôle de vos fonds en Ethers en permanence, sauf au moment où vous misez. Nous pouvons aussi fournir des outils qui garantissent que la donne est juste (car parfois il y a de la triche sur ce genre de jeux en ligne)[34] », précise Joseph Lubin. Toutefois Etherpoker, qui n'est pas la priorité de Consensys, est encore loin de pouvoir être commercialisé.

Le domaine des paris est aussi transformé par les applications blockchain. BitBet.us, créé dès 2013 et revendu en février 2016 à une personne qui opère sous le pseudonyme de Znort987, y fait figure de précurseur. Sur BitBet.us, les utilisateurs parient anonymement en Bitcoin sur les questions les plus diverses, souvent relatives à l'actualité financière ou politique, qu'ils ont eux même suggérées : est-ce que la valeur du Bitcoin dépassera 1 000 dollars au 1er janvier 2017 ? Est-ce que le Nevada va légaliser la marijuana en 2016 ? Est-ce qu'Hillary Clinton sera élue présidente des États-Unis ? Est-ce qu'elle sera mise en examen avant le 1er janvier 2017 ? Etc. « Les principaux avantages de notre système [par rapport à un site de paris classique] sont le transfert quasi instantané de la valeur entre les utilisateurs et le site, la garantie apportée par la blockchain que BitBet opère de manière honnête et éthique (toutes les transactions entrantes et sortantes sont 100 % visibles par le monde entier) et enfin l'anonymat[35] », a accepté de répondre l'équipe de BitBet.us [*14]. « Nous nous considérons comme un outil que les gens peuvent utiliser pour débattre de leurs désaccords sur ce que sera le futur, d'une manière équitable et non biaisée […] et aussi comme une manière de s'amuser en pariant ou en créant des paris », ajoutent-ils.

Deviner l'avenir

Dérivés de ces applications de pari, plusieurs projets se sont lancés sur le concept neuf et prometteur de « marché prédictif » : une manière de deviner avec une plus grande fiabilité l'avenir en mobilisant l'intelligence des masses, par le biais de paris de très nombreux utilisateurs, qui finissent par former un consensus sur une question donnée. C'est l'ambition d'Augur, une start-up américaine qui fait partie des plus en vue dans le secteur de la blockchain. Influencés par les théories économiques libérales, les créateurs d'Augur conçoivent le futur comme un marché et le prix comme un élément d'information décisif sur l'état de ce marché. « Augur a été inspiré par plusieurs grandes idées, dont le travail du philosophe et économiste autrichien Friedrich von Hayek[*15] », explique Peronet Despeignes, responsable des opérations spéciales chez Augur. « Il a notamment écrit *L'Utilisation de la connaissance dans la société* (1945), où il insiste sur l'importance des prix dans l'économie, qui sont pour lui des outils de communication (pour indiquer les pénuries ou les surplus par exemple) et où il décrit les marchés comme des systèmes de communication, où les acheteurs et les vendeurs se transmettent des informations », ajoute-t-il. Au concept de prix comme indicateur d'information, les fondateurs d'Augur ont ajouté celui de « sagesse de la foule », défini par le journaliste du *New Yorker* James Surowiecki, dans un ouvrage paru en 2004. « Il y fournit un grand nombre d'exemples où les marchés ont fonctionné comme d'excellents indicateurs du futur », note Peronet, pour qui « le marché motive les gens, par le profit, à révéler ce qu'ils savent ou ce qu'ils croient qu'il va advenir ». Enfin, s'ajoutent à ce corpus théorique les travaux du mathématicien et économiste John Forbes Nash[*16] sur le point d'équilibre : « Si vous donnez rendez-vous à des gens à New York, sans préciser où exactement, ils vont spontanément se concentrer sur quelques lieux, comme la statue de la Liberté ou l'Empire State Building », illustre Peronet Despeignes. Placés devant la même interrogation – où y a-t-il le plus de chance que l'on se retrouve ? –, les participants vont faire des prédictions qui vont naturellement se rejoindre pour former un consensus autoréalisateur (tout le monde décide d'aller aux quelques endroits où tout le monde avait prévu que le plus de monde irait). Voilà pour les théories, assez passionnantes, sur lesquelles reposent les projets d'Augur.

Concrètement, le site, toujours en version bêta à l'automne 2016, prend la forme d'une plateforme entièrement décentralisée où se succèdent des paris proposés par les utilisateurs, sur lesquels chacun peut miser, signant alors un *smart contract* sur la blockchain Ethereum. Par exemple : « Est-ce que Novak Djokovic sera numéro 1 mondial de tennis fin 2016 ? » Les gens achètent des actions « oui » ou des actions « non », dont le prix gravite entre 0 (si les parieurs jugent que la prédiction n'aura pas lieu) et 1 (s'ils sont confiants dans le fait qu'elle aura lieu). À la fin de l'année 2016, un certain nombre de participants volontaires (un groupe de 2 000 rapporteurs qui ont investi dans l'achat de jetons Augur à l'automne 2015) indiquent le résultat : l'événement a eu lieu, ou n'a pas eu lieu, ou le résultat ne peut pas être déterminé[*17]. Les gagnants se partagent la mise, sur laquelle sont prélevées deux commissions : une pour les rapporteurs et une pour la personne qui a créé le pari (qui n'est en revanche pas récompensée si sa question a été mal formulée au point qu'elle n'a pas pu avoir de réponse claire). La plateforme ne prélève aucune commission pour elle-même. Ses fondateurs gagnent de l'argent en s'inscrivant comme rapporteurs des événements et n'exercent aucun contrôle sur Augur, qui est entièrement décentralisé. À ce

jour, la plateforme, encore en version bêta, n'est pas opérationnelle : tant que toutes les vérifications de sécurité prévues par Augur n'auront pas été réalisées, les paris continueront à avoir lieu avec de l'argent fictif. L'enjeu de sécurité est décisif, car des sommes très importantes devraient plus tard y circuler. À long terme, les ambitions d'Augur sont immenses : « Nous voulons créer un système d'alerte pour tout, un GPS pour s'orienter dans la vie. Par exemple, pour accélérer la diffusion de l'information en cas de catastrophes naturelles. Imaginons qu'un amateur australien soit hyperbon pour anticiper les tremblements de terre et devine qu'il devrait s'en produire un à l'autre bout du monde, au Chili, dans les deux prochaines semaines. Il ouvre un marché prédictif, afin que le public en soit averti. Nous créons une plateforme où la diffusion du savoir est ouverte à tous, pas seulement aux experts », s'enthousiasme-t-il. Bien que le système soit encore à un stade expérimental, il a déjà réussi à prévoir quelques événements inattendus, comme la victoire des partisans du Brexit (la sortie de la Grande-Bretagne de l'Union européenne) alors que les sondages classiques donnaient le maintien dans l'Union gagnant.

Service prometteur, les marchés prédictifs intéressent également Consensys, qui a développé l'application Gnosys. Joseph Lubin la définit comme « une plateforme où créer des marchés prédictifs, et un excellent outil pour mobiliser la sagesse de la foule ». Pourquoi l'avenir serait-il mieux prédit avec ce type de système ? « Si on demande leur avis à 50 personnes sur un événement futur, il y a une bonne chance qu'ils trouvent la bonne réponse », résume Simon Polrot, qui suit de près les projets de Consensys sur son site Ethereum France. « C'est comme un sondage sur la blockchain, avec un aspect d'investissement monétaire qui oblige les sondés à répondre sérieusement[36] », ajoute-t-il. Ces applications rencontreront-elles le succès espéré ? Les paris sont ouverts !

---

*1. Ou serveurs.

*2. Rchain, qui fonctionne avec un système de validation *proof of stake*.

*3. En 2015, Airbnb a versé 69 128 euros d'impôts au fisc français. En 2014, Uber aurait versé 400 000 euros.

*4. L'entreprise a beaucoup fait parler d'elle en étant à l'origine de l'aventure malheureuse de TheDAO.

*5. C'est-à-dire d'hébergement à distance de fichiers ou de logiciels, qui n'ont plus besoin d'être stockés sur votre ordinateur.

*6. L'adresse IP du créateur peut également être intraçable, en utilisant le réseau Tor.

*7. « Deviens riche ou meurs en essayant. »

*8. Avec les pistes des différents instruments séparées.

*9. La capacité à supporter une large demande.

*10. Une plateforme de financement collaboratif.

*11. Ou du moins pense l'être, et c'est bien le problème !

*12. Journalisme participatif.

*13. Aux États-Unis.

*14. Sous couvert d'anonymat, précisément.

*15. Prix Nobel d'économie 1974 pour ses travaux sur la monnaie.

*16. Prix Nobel d'économie 1994, rendu célèbre par le film *Un homme d'exception*, avec Russell Crowe.

*17. En l’occurrence, Novak Djokovic n’est plus numéro 1 mondial, il a été dépassé par son rival écossais Andy Murray.

CHAPITRE 6

Un tremplin vers un monde automatisé

Il y a eu les ordinateurs connectés à Internet, au milieu des années 1990. Puis les téléphones connectés, à partir du milieu des années 2000. Les montres connectées, qui ont connu de premiers succès commerciaux à partir de 2013. Et ensuite les bracelets connectés, les lunettes connectées, les réfrigérateurs connectés, les voitures connectées, les cafetières connectées, les chaussures connectées, les skis connectés, les drones (connectés, cela va sans dire), les équipements de santé connectés, les toilettes connectées et même les préservatifs connectés. Petit à petit, tout se connecte. Selon une étude du cabinet Gartner, publiée fin 2015, 4,9 milliards d'objets connectés étaient déjà en circulation et 20,8 milliards le seront en 2020[1]. L'institut européen Idate va plus loin encore et estime que le monde en comptera, en 2025, 155 milliards[2]. Ces innombrables objets en tous genres produisent des données, qui sont pour l'instant stockées sur des serveurs. Ils sont parfois également capables d'échanger des informations entre eux (de votre smartphone à votre télévision par exemple). Là encore, ces communications passent par des serveurs. Le volume de données à traiter explose, il n'est pas facile de traiter toutes ces interactions. « Avec la multiplication des objets connectés, on ne pourra pas gérer tous ces flux d'information[3] », souligne Éric Lévy-Bencheton, de Keyrus. À moins de décentraliser et d'automatiser ces échanges dans des *smart contracts* inscrits sur une blockchain. « Aujourd'hui, tous ces objets communiquent à un serveur central, qui traite les informations, décide des réactions et les renvoie aux machines. Celles-ci ne peuvent pas vraiment faire de transactions directement entre elles. Avec la blockchain, les objets connectés peuvent interagir en pair à pair, communiquer entre eux et faire des transactions[4] », insiste Primavera De Filippi, chargée de recherche au CNRS et au Berkman Center for Internet and Society, de l'université d'Harvard – et ce tout en bénéficiant des avantages de ce type de système : « La transparence, l'immutabilité et la garantie des exécutions », ajoute-t-elle. « Comme le nombre d'objets connectés va devenir très important, ce serait intéressant de les laisser se coordonner entre eux pour prendre des décisions, plutôt que de leur donner des ordres de manière verticale. C'est ce qu'on a appelé la démocratie des objets[5] », abonde Luca Comparini, responsable blockchain chez IBM France.

Logiquement, ces deux dernières années, tous les secteurs qui s'intéressent à l'automatisation permise par l'interaction des objets connectés (géants de l'énergie, de l'automobile et industriels en tous genres, etc.), se sont pris de passion pour la blockchain. Des registres distribués, transparents et sécurisés pourraient en effet être l'élément qui manquait pour organiser une économie véritablement automatisée de bout en bout : de la production d'un bien jusqu'au service qu'il apporte au client final, en passant par son acheminement, sa commercialisation, sa distribution (et même son éventuel remboursement en cas de sinistre, comme on l'a vu dans le chapitre consacré à l'assurance). La blockchain serait alors le tremplin vers un monde robotisé, où l'homme n'aurait plus grand-chose à faire, pour le meilleur ou pour le pire. Ce grand bouleversement a déjà commencé. Installez-vous bien confortablement dans votre fauteuil : vous n'aurez peut-être bientôt plus besoin d'en bouger.

Le ballet autonome des objets connectés

La machine à laver a libéré les hommes et les femmes de l'ingrate tâche de la lessive. Voilà qu'elle promet maintenant de les libérer même de l'achat de détergent. En janvier 2015, au Consumer Electronics Show (CES) de Las Vegas, le plus grand salon mondial de l'électronique, IBM et Samsung dévoilaient un prototype surprenant de machine à laver connectée classique, la Samsung W9000, reconfigurée pour pouvoir commander elle-même la lessive dont elle a besoin, grâce à un protocole blockchain d'IBM baptisé Adept. « C'est le premier prototype qu'on a dévoilé au grand public, en partenariat avec Samsung. Cette machine à laver connectée pouvait s'approvisionner en savon quand son réservoir était presque vide, et déclencher l'intervention d'un technicien agréé en cas de panne. Elle pouvait aussi se mettre en lien avec les autres objets connectés de l'immeuble pour déterminer les meilleures plages horaires d'utilisation, afin d'optimiser la consommation d'énergie dans l'immeuble. Tout cela grâce à des *smart contrats* hébergés et exécutés dans la blockchain », indique Luca Comparini, d'IBM France. Plus anecdotique qu'autre chose, cette expérience a eu le mérite d'illustrer, de manière concrète, les possibilités d'automatisation offertes par l'alliance des objets connectés et de la blockchain, qui sont aussi nombreuses que puissantes.

L'automobile en première ligne

De nombreux projets, plus avancés, ont été lancés dans le secteur de l'automobile, qui prépare l'arrivée massive des véhicules autonomes, annoncée pour 2020. Plusieurs utilisations sont envisagées, en particulier la recharge automatique en énergie (achat d'essence ou d'électricité). Outre-Rhin, la start-up Slock.it y travaille avec Innogy, une filiale du géant allemand RWE. « On développe un système où les véhicules se rechargent tout seuls au feu rouge, grâce à une plaque à induction placée dans la voiture et une autre sous la route », confie Stephan Tual. « Les deux plaques fonctionnent comme deux antennes :

l'une charge la voiture, l'autre reçoit l'énergie. Le portefeuille de la voiture paye la route pour avoir de l'électricité (quelques dixièmes de centimes pour un peu de courant). Sans blockchain, il faudrait faire une connexion à un serveur de paiement centralisé, qui prendrait du temps et coûterait de l'argent. Avec la blockchain, c'est gratuit et immédiat », s'enthousiasme-t-il. Les perspectives de tels systèmes, s'ils étaient généralisés, sont vertigineuses : « Ça permet en théorie d'avoir des véhicules électriques qui n'auront jamais à s'arrêter, sauf pour la maintenance », note-t-il. De quoi intéresser les particuliers, mais aussi les grandes entreprises de la logistique, qui pourraient limiter les interruptions des processus de livraison et accélérer le transport. Au fil de leurs recherches, les équipes de Slock.it et RWE ont fait évoluer leur idée : « À la base, on envisageait des bornes de chargement statique, mais on réfléchit maintenant à un modèle pair à pair : les bornes de chargement seraient devant les maisons de particuliers, qui rentabiliseraient leur investissement en louant l'accès à leur borne à d'autres usagers », précise Stephan Tual. « Les crédits gagnés en échange de cette mise à disposition pourraient être utilisés pour régler un autre service, comme des taxis autonomes », suggère-t-il.

Comme la voiture autonome, potentiellement tous les objets connectés pourraient commander leur énergie en passant des transactions automatisées sur une blockchain. « J'ai 10 radiateurs connectés chez moi, je veux qu'en hiver il fasse 14 degrés la nuit et 20 degrés la journée. Les radiateurs peuvent écrire un *smart contrat*, lancer un appel d'offres sur une plateforme d'énergéticiens, spécifiant qu'ils ont besoin de tant de kilowatts de telle heure à telle heure, et choisir automatiquement le mieux-disant du marché[6] », imagine le Français Alain Brégy, cofondateur d'Aedeus, une PME spécialisée dans l'utilisation de la blockchain pour sécuriser les communications entre objets connectés.

La blockchain pour sécuriser les échanges

Si l'on remet notre destin entre les mains d'objets connectés, mieux vaut être certain que le système est sûr, n'a pas de faille et ne peut pas être hacké. Des voitures autonomes l'ont déjà été, ce qui pose de graves problèmes de sécurité. Heureusement, la blockchain peut servir d'outil pour garantir l'intégrité des communications entre objets connectés, comme l'explique Martin Ruubel, qui dirige les activités de « gouvernement numérique » chez Guardtime[*1]. « Si vous possédez une voiture autonome, c'est comme si vous rouliez dans une arme meurtrière que vous ne contrôlez pas[7] », lance-t-il, provocateur. « Il est de la plus haute importance que chaque système utilisé à l'intérieur et à l'extérieur de cette voiture ne soit pas corrompu ou hacké. Vous voulez être certain que le véhicule autonome ne fera fonctionner que les logiciels prévus, comme il était prévu qu'ils fonctionnent. La blockchain permet de vérifier en continu que le système à l'intérieur de votre voiture fonctionne correctement. Et si quelque chose se passe, il permet de comprendre ce qui s'est passé, qui a fait quoi et quand, comme une boîte noire pour un avion », insiste l'expert estonien, qui précise au passage que Guardtime collabore actuellement avec deux constructeurs automobiles et un sous-traitant spécialisé dans les composants électroniques. La sécurisation des échanges entre objets connectés est un enjeu commercial énorme. IBM a lancé une offre de stockage des données des objets connectés sur une blockchain privée (Hyperledger) associée à sa

plateforme dédiée à l'Internet des objets, Watson IoT. Preuve de l'importance stratégique de ce service, l'entreprise a annoncé un investissement de 200 millions de dollars pour développer Watson IoT sur son site de Munich, début octobre 2016. Cette décision laisse également présager des associations futures entre blockchain et intelligence artificielle (pour laquelle le robot Watson d'IBM s'est rendu célèbre).

L'arrivée des organisations autonomes décentralisées

Jusqu'où ira l'interconnexion des objets sur la blockchain ? Sa logique pousse à la création d'organisations entièrement autonomes et décentralisées, que les experts du secteur appellent des DAO (*distributed autonomous organisations*) : des entités complètement décentralisées, régies par un programme informatique inscrit dans la blockchain[*2], qui exécute, de manière automatique, transparente et immuable, les règles de gouvernance acceptées par les membres. Une première DAO avait été créée par Stephan Tual et ses associés de Slock.it, sous la forme d'un fonds d'investissement collaboratif. « Transposées aux objets connectés, ces DAO, des entités algorithmiques, permettent de créer des robots autonomes qui sont dotés de leur propre logique gérée par la blockchain, et capables de gagner de l'argent pour acquérir ensuite leurs propres ressources[8] », commente Primavera De Filippi, chargée de recherche au CNRS et au Berkman Center for Internet and Society, de l'université d'Harvard. Sur ce principe, les applications sont infinies. La chercheuse, également artiste, a ainsi créé une œuvre qui se veut « une illustration artistique du principe de la DAO ». Baptisée *Plantoïde*, cette installation, conçue avec trois autres artistes et experts de la blockchain (David Bovill, Vincent Roudaut, Sara Renaud), est une plante robot autosuffisante, qui finance sa propre reproduction en faisant appel aux dons du public. Les spectateurs peuvent la « nourrir » en lui envoyant, sur la blockchain, des Bitcoins. « Quand suffisamment d'argent est récolté, la plante lance un appel d'offres. Les gens peuvent soumettre des propositions sur la création d'une nouvelle plateforme, et les contributeurs peuvent voter. Quand un gagnant est trouvé, l'argent est transféré à un artiste qui aura la charge de créer une nouvelle plantoïde », explique Primavera De Filippi.

Une illustration inventive du concept de DAO, qui pourrait bien être utilisé à l'avenir à des fins moins poétiques. Par exemple pour automatiser, de bout en bout, un processus logistique entier. « Imaginons que j'aie besoin de 1 000 pièces jaunes en plastique d'une certaine taille », suppose Alain Brégy, d'Aedeus. « Quand le camion connecté va être géolocalisé sur le site de production, un capteur va me dire qu'il fait 200 kg de plus et qu'il quitte le lieu. Je peux considérer que la matière première a été chargée. Le système paye donc instantanément le producteur de matière première, sans que personne n'intervienne. Quand le camion dépose la marchandise dans l'usine où est la machine-outil, il a 200 kilos de moins. Le paiement du transporteur a lieu. Quand le compteur de la machine atteint 1 000 pièces, la machine est rémunérée elle aussi. Elle informe le système qu'elle a consommé tant de kilowatts, et l'énergéticien est réglé. Puis le transporteur revient. Il charge les pièces, les livre à l'endroit prévu et est payé à son tour. Finalement, j'ai monté ainsi une entreprise temporaire, sans numéro de Siret ni employé, qui ne dure que le temps de l'ensemble des transactions qu'elle doit résoudre. »

Avant d'en arriver là, de véritables entreprises, à l'ancienne, comptent déjà mettre à profit la blockchain pour automatiser encore plus leurs processus logistiques. IBM y travaille pour ses clients et a dévoilé un projet dans l'industrie du bois, lors de sa conférence annuelle Interconnect à Las Vegas, en février 2016. « On s'est intéressés à une ville en Finlande, qui a l'ambition de devenir le grand hub de transport de l'industrie du bois », confie Luca Comparini. « Ils sont dans une position stratégique, entre l'Europe et l'Asie, et disposent d'un port important et d'une gare très proches », poursuit-il. « Pour eux, l'association de la blockchain et des objets connectés peut offrir une meilleure transparence dans la traçabilité des conteneurs du bois, afin d'être plus efficaces dans les plannings et l'exécution des tâches. Savoir exactement quand un conteneur va arriver permet d'optimiser toute la chaîne de valeur qui suit, du transport à la production. Sur le même principe, il existe aussi d'autres applications possibles dans l'agroalimentaire, pour assurer la traçabilité d'un transport où la chaîne du froid ne doit pas être rompue, par exemple. »

ÉNERGIE : TOUS BRANCHÉS SUR SON VOISIN

Dans le secteur de l'énergie, trois catégories de projets innovants, fondées sur des blockchains, sont actuellement expérimentées. Il y a d'abord l'association de cette technologie aux compteurs intelligents (*smart meter*), qui pourront, au lieu de simplement mesurer votre consommation, acheter l'énergie dont vous avez besoin, voire la revendre si vous avez un panneau solaire sur le toit de votre immeuble. Ensuite, différentes initiatives incitent à la production et à la consommation d'électricité renouvelable, par la création de jetons (ou *tokens*, en réalité, une somme en cryptomonnaie) permettant spécifiquement l'acquisition d'énergie propre. Enfin, l'alliance de ces deux innovations offre la possibilité de donner naissance à de véritables réseaux d'énergie décentralisés (*smart grids*) : des systèmes où chaque habitation, consommatrice et éventuellement productrice d'électricité grâce à un panneau solaire ou une mini-éolienne, calcule en temps réel l'énergie dont elle a besoin, à l'aide de son compteur intelligent, puis achète ou revend le solde en jetons de cryptomonnaie à ses voisins. Tout cela automatiquement et en toute transparence, par l'intermédiaire de *smart contracts* inscrits dans la blockchain.

Cryptocompteurs intelligents

Progressivement installé dans les foyers français depuis le 1er décembre 2015, le compteur intelligent Linky, d'Enedis (ex-ERDF), a familiarisé le grand public avec cette technologie. L'étape suivante est de connecter ce type d'engins à une blockchain. La start-up française Stratumn y travaille. Objectif : utiliser ces registres distribués pour permettre de contrôler en temps réel la consommation de chacun. La blockchain offre en effet la plateforme idoine où enregistrer, de manière transparente, irrévocable et opposable, les volumes consommés. Un tel système permettrait, par exemple, d'éviter la

surconsommation dans les grandes copropriétés, où la facture énergétique est mutualisée. L'affichage en temps réel donne aussi au client la possibilité de mieux évaluer sa consommation et de la réguler (évitant les mauvaises surprises que beaucoup ont un jour connues quand arrive la facture). Appliquée par Stratumn à l'électricité, l'alliance de la blockchain et des compteurs intelligents peut trouver son utilité pour n'importe quel autre flux, par exemple la consommation et la distribution d'eau. Le géant français Engie a ainsi mené une première expérimentation dans l'Yonne : un réseau de capteurs connectés, relié à une blockchain bâtie sur le modèle d'Ethereum, appelle automatiquement un dépanneur en cas de fuite. « Quand un compteur d'eau détecte un problème d'écoulement de l'eau, il contacte et passe un contrat avec un service de maintenance[9] », explique Étienne Gehain, responsable R&D du projet, selon un article des *Échos* de juin 2016. Tout a lieu sans intervention humaine, selon les conditions établies dans un *smart contract*, inscrit dans la blockchain. « Le responsable R&D aurait pu passer par une solution centralisée, à l'inverse d'une blockchain. Mais les blockchains pourraient être bien moins chères que l'informatique standard à l'avenir », précise l'auteur de l'article.

En Afrique du Sud, une autre start-up, Bankymoon, a mis en place, au printemps 2016, une initiative originale et solidaire, baptisée Usizo, utilisant elle aussi compteurs intelligents et blockchain. Usizo est une plateforme de financement participatif, sur laquelle n'importe qui peut déposer un don, en Bitcoins, pour participer au paiement des factures d'électricité de différentes écoles défavorisées en Afrique du Sud, notamment dans le quartier de Soweto, à Johannesburg. Ces écoles sont équipées de compteurs intelligents, reliés à une blockchain, ce qui leur permet de recevoir les fonds pour commander et recevoir l'énergie dont le bâtiment a besoin. Assez révolutionnaire, ce concept permet de désintermédier l'action humanitaire. Plus besoin d'ONG : « Vous pouvez maintenant avoir un compteur intelligent, relié à la blockchain Bitcoin, qui reçoit directement l'argent de donateurs étrangers sans passer par une organisation qui pourrait prendre ou redistribuer ces fonds[10] », souligne le PDG de Bankymoon, Lorien Gamaroff, dans un article du site spécialisé CoinDesk.

Des jetons pour valoriser les énergies renouvelables

Dès le début de l'année 2014, alors que personne ou presque n'utilisait encore le mot « blockchain », la première monnaie virtuelle écologique est née : le SolarCoin, une devise créée pour récompenser la production d'énergie propre. Son principe est simple : chaque mégawatt/heure d'énergie photovoltaïque produit permet à son producteur de gagner un SolarCoin (après validation du système de production par les membres bénévoles de la fondation SolarCoin, authentification du générateur et vérification du compteur). Le SolarCoin est ainsi l'équivalent d'un certificat d'origine, mais qui serait doté d'une valeur marchande, puisqu'il peut être cédé et échangé sur différentes plateformes contre d'autres cryptomonnaies ou même des devises traditionnelles. Ce système permet de créer un véritable marché de l'énergie solaire, ouvert à tous. Les producteurs ont tout à y gagner : le SolarCoin s'ajoute à l'argent qu'ils retirent de la vente de l'électricité produite, et permet ainsi de rentabiliser plus vite l'achat

de l'équipement en panneaux solaires. À condition toutefois que la devise prenne un peu de valeur sur les plateformes d'échange, car au 14 janvier 2017, un SolarCoin s'échangeait contre 0,06 dollar[11].

Les transactions de SolarCoins ont lieu sur une blockchain dédiée : ElectriCChain, qui enregistre à la fois les transactions et les données de production d'énergie propre de ses utilisateurs, qui pourront servir aux scientifiques ou aux météorologues. D'ici quinze à vingt-cinq ans, ElectriCChain a pour objectif d'accueillir dans son réseau les quelque 7 millions d'installations de panneaux solaires qui existent dans le monde, et d'y raccorder pas moins de 200 millions de foyers résidentiels, qui pourront ainsi acquérir ou revendre des SolarCoins. En août 2016, plus de 85 000 MWh d'énergie solaire produits avaient déjà été récompensés par des SolarCoins, dans 21 pays différents. Plusieurs grandes institutions se sont déjà associées au projet, comme le MIT et la Nasa. Plus récemment, la plateforme de financement participative française Lumo, spécialisée dans le soutien aux projets de production d'énergie renouvelable, a également rejoint ElectriCChain, afin que ses investisseurs puissent recevoir des SolarCoins en récompense de leur action. En octobre, Lumo a gratifié un premier projet et distribué « des SolarCoins à 50 investisseurs qui ont cofinancé en 2013 une centrale photovoltaïque de 36 kW sur une école primaire à Aytré, près de La Rochelle[12] », selon *Environnement magazine*.

Les SolarCoins ne sont toutefois pas seuls à vouloir servir de monnaie d'échange à la production d'énergie. D'autres projets se préparent, comme EcoCoins, un concept de monnaie numérique visant à utiliser la blockchain Bitcoin pour construire une place de marché où particuliers et entreprises pourraient acheter et revendre de l'énergie propre. Mis au point par une équipe germano-américaine, il a été récompensé en octobre 2016 par le premier prix d'un hackathon (un concours de développeurs) organisé par la filiale néerlandaise d'Engie (Hack 4 Energy).

Une chance pour les microréseaux d'énergie propre

Prenez des compteurs intelligents, une blockchain et une cryptomonnaie représentant de l'énergie propre, définissez un périmètre, raccordez le tout… Voilà la recette du *smart grid* de demain : un réseau décentralisé de production et de distribution d'énergie renouvelable. De toutes les perspectives qu'ouvre la blockchain, celle-ci est l'une des plus enthousiasmante. Les *smart grids*, ces systèmes où le panneau solaire d'une maison peut alimenter en énergie celle du voisin, ou l'inverse en fonction de la production et de la consommation de chacun, existaient avant la blockchain. Mais cette technologie permet de décentraliser réellement ces réseaux, qui peuvent ainsi s'émanciper de la tutelle d'un grand énergéticien : l'investissement de chacun dans un panneau solaire ou une mini-éolienne est alors plus facilement rentabilisé. De plus, la blockchain offre une structure idéale pour organiser des transactions instantanées, sécurisées et transparentes au sein d'une communauté. Elle est peut-être le tremplin qui manquait pour permettre l'essor de ces microréseaux d'énergie propre. Deux projets précurseurs, menés respectivement à Brooklyn et à Lyon, dans le quartier de la Confluence, en 2016, prouvent l'intérêt qui y est porté à ce type d'usage.

Pionnier souvent pris en exemple dans le secteur, Transactive Grid est un microréseau de consommateurs et de producteurs d'énergie solaire, inauguré en mars 2016 dans deux quartiers de Brooklyn (Park Slope et Gowanus) à New York, par les sociétés Consensys et Lo3 Energy. Ces deux quartiers n'ont pas été choisis par hasard. « La production a lieu à Park Slope, une aire résidentielle, où les couples de hipsters élèvent leurs enfants. Beaucoup de gens y ont des panneaux solaires. À côté, Gowanus est une zone industrielle, et va le rester (car elle est très polluée depuis l'ouragan Sandy). C'était donc un parfait endroit pour le stockage de l'énergie », note John Lilic, en charge du projet chez Consensys. Un tel système présente deux grands avantages : l'aspect écologique bien sûr, mais aussi la résilience. « Prenez un hôpital. Vous voulez être certain qu'en cas de coupure de courant, il pourra encore fonctionner. Vous pouvez renforcer son autonomie en l'inscrivant dans un réseau distribué. » Si une tempête, comme l'ouragan Sandy qui a ravagé New York en 2012, entraîne une coupure de courant dans la ville, le microréseau peut continuer à alimenter le quartier. Au sein de Transactive Grid, les habitants membres, à la fois consommateurs et producteurs, ont le contrôle de leur propre marché d'échange de l'énergie, sur lequel chacun achète ou vend sa production, en passant des transactions sur la blockchain Ethereum. « Si vous produisez plus que vous ne consommez, le surplus est distribué dans le réseau et peut être consommé par vos voisins », résume John Lilic. Auparavant, les particuliers qui produisaient de l'énergie étaient dans l'obligation de la céder à une grande compagnie. « Mais celle-ci ne vous paye pas l'intégralité de la valeur de ce que vous avez produit. À New York vous en touchez environ 50 %. Vous ne faites pas une bonne affaire. C'est pourquoi nous avons voulu changer ce *business model* », insiste-t-il. « Avec Transactive Grid, chaque membre est connecté à un compteur intelligent, qui calcule votre consommation et votre production. Le surplus génère des jetons numériques, que vous pouvez échanger au sein du réseau Ethereum. Vous pouvez acheter mes jetons qui représentent ma capacité de production d'énergie », explique l'expert. En réalité, vous n'achetez donc pas directement l'énergie du voisin, mais un crédit qui représente l'énergie du voisin. « C'est juste un prototype », admet-il (qui fonctionne néanmoins), car l'expérience a une limite : il faut un énergéticien pour assurer la distribution de l'électricité produite dans le réseau. Pour cette raison, Consensys travaille avec le groupe allemand RWE (qui a la capacité de distribuer le courant) pour développer à plus large échelle ces systèmes, dans le cadre d'une initiative appelée Co-tricity. « Avec Co-tricity, nous créons une plateforme où les producteurs-consommateurs d'énergie peuvent vendre les jetons, correspondant à leur production, à des PME locales (une épicerie par exemple). Ces PME peuvent ensuite céder leurs jetons à RWE, qui leur distribue du courant en échange. C'est une manière d'acheter de l'énergie solaire générée par la communauté », explique-t-il. Ce projet, encore en phase de développement, pourrait se concrétiser dès le début de l'année 2017.

En France, une initiative très semblable a vu le jour à l'automne 2016. Le 28 juillet 2016, une ordonnance gouvernementale relative à l'autoconsommation d'énergie ouvrait la voie aux microréseaux pilotés sur la blockchain. À peine trois mois plus tard, le promoteur Bouygues Immobilier et la start-up Stratumn annonçaient leur projet commun de mini-*smart grid* décentralisé sur une blockchain privée. Situé dans le quartier de la Confluence, à Lyon, il permettra aux habitants d'échanger l'énergie solaire

qu'ils auront produite et voudront consommer, en pair à pair. Ce prototype se veut un « démonstrateur d'un réseau local décentralisé de supervision des échanges d'énergie[13] », selon Bouygues Immobilier. « Nous voulons permettre aux habitants d'un écoquartier de bénéficier d'une énergie solaire d'origine certifiée, provenant de panneaux photovoltaïques dans le voisinage du consommateur[14] », explique Olivier Sellès, responsable innovation énergie et *smart grids* chez Bouygues Immobilier, au site L'Usine digitale. « Aujourd'hui, on peut déjà souscrire un abonnement pour consommer plus d'énergie verte, mais en réalité, il n'existe aucune possibilité de tracer l'origine de l'électricité. Donc on peut acheter du nucléaire sans le savoir. Avec la blockchain, on apporte une preuve de l'origine de l'énergie achetée[15] », insiste François Dorléans, de Stratumn. Un premier système pilote commencera en 2017. « À terme, ça pourrait être fait à grande échelle », s'enthousiasme le jeune expert.

Produire en toute transparence

Consultable par tous ses membres, quasiment impossible à modifier, la blockchain constitue aussi un registre fiable où toutes les parties prenantes d'un processus de production peuvent inscrire des informations à chacune de ses étapes, pour garantir une traçabilité totale au produit final. Qu'il s'agisse d'extraction de diamant, de tests préparatoires à la mise sur le marché d'un médicament ou de l'assemblage d'un Airbus A380, toutes les industries où l'origine de la matière première et le processus de production sont des enjeux décisifs, pour des raisons de sécurité ou d'éthique, peuvent trouver dans la blockchain un outil idéal pour graver dans le marbre l'historique de leur produit. Celle-ci sert de base de données partagée et décentralisée, dans laquelle tous les participants (clients, fournisseurs, producteurs, régulateurs) peuvent avoir confiance puisqu'aucun d'entre eux n'a de contrôle sur celle-ci, ni de possibilité de la corriger. Si une défaillance technique survient, les informations enregistrées peuvent être auditées pour en trouver l'origine et fournir les explications nécessaires au régulateur, au consommateur ou au client qui les exigent. De nombreuses PME ont lancé ce type d'applications de « notarisation » (enregistrement de données opposables). Stratumn, par exemple, a développé Chainscript, « un rail d'audit cryptographique qui permet de retracer tous les points d'un *business process* », explique François Dorléans. Des grands noms des secteurs les plus divers se sont montrés intéressés : laboratoires pharmaceutiques (pour les essais cliniques), mais aussi des industriels de l'aéronautique ou du ferroviaire… « Sur ce type de projets très complexes, avec des millions de pièces, beaucoup de documentation technique et plusieurs vérifications, il faut pouvoir partager la donnée de façon propre avec les entreprises partenaires[*3], pour pouvoir retracer l'origine du moindre problème », explique François Dorléans. « En cas de crash aérien, on va pouvoir savoir qui a fabriqué la pièce défaillante et si elle a été montée selon les règles de l'art », précise le consultant Éric Lévy-Bencheton, de Keyrus. « Aujourd'hui, il existe déjà des registres de fabrication dans l'automobile ou l'aéronautique, ajoute-t-il, mais ils sont tenus par les constructeurs eux-mêmes. La blockchain est une solution plus fiable, car le constructeur ne peut pas altérer l'information pour se dédouaner de sa responsabilité. » En dehors de

l'industrie lourde, deux secteurs se sont montrés particulièrement en pointe dans le développement de ce type de solutions : la santé et le diamant. Aussi différents soient-ils, ils partagent tous deux une même problématique : la nécessité éthique et légale de pouvoir retracer très précisément l'origine et le parcours de leur produit.

La blockchain au service de la recherche médicale

En janvier 2016, un patient décédait lors de l'essai clinique d'une nouvelle molécule antalgique (BIA 10-2474), mené à Rennes par le centre de recherche Biotrial pour le compte du laboratoire portugais Bial. Quatre autres participants à ce programme ont souffert de lésions cérébrales. Depuis, une enquête de l'Inspection générale des affaires sociales a relevé plusieurs manquements majeurs dans la conduite de l'essai par le centre de recherche et dans sa réaction après l'accident. Tous sont relatifs à un manque d'information ou de transparence : Biotrial se voit reprocher de s'être informé trop tard de l'état de santé du patient hospitalisé, de ne pas avoir arrêté l'administration du produit aux autres participants et de ne pas les avoir informés du problème survenu au premier volontaire ; enfin, de ne pas avoir informé immédiatement les autorités sanitaires[16]. Avec la blockchain, un tel dysfonctionnement aurait pu être évité. Dans une telle affaire, décrire chacune des étapes de l'essai, à mesure qu'elles ont lieu, dans un registre commun observable par tous les acteurs (le centre de recherche qui fait les tests, le laboratoire qui les commande, les autorités sanitaires qui les autorisent, voire les patients qui les subissent) aurait permis de les avertir du problème tout de suite, de prendre la décision d'interrompre l'essai plus tôt et d'établir les responsabilités de chacun plus clairement et plus vite.

Start-up de la santé et grands groupes pharmaceutiques se penchent sérieusement sur cette question. « Il existe déjà au moins un laboratoire de recherche médicale, dont le nom doit rester confidentiel, qui utilise une blockchain pour certifier ses processus d'essais cliniques sur des humains », glisse Éric Lévy-Bencheton, de Keyrus. En France toujours, Stratumn travaille avec un hôpital parisien sur l'enregistrement sur la blockchain des phases de tests cliniques de nouveaux médicaments : « Tous les intervenants pourront suivre en temps réel chaque action et chaque événement médical affectant des dizaines de milliers de patients. En même temps, grâce au cryptage, les données confidentielles des patients pourront être protégées[17] », a déclaré le fondateur de Stratumn, Richard Caetano, au journaliste du *Monde* Yves Eudes.

Quelques mois plus tôt, en mai 2016, deux médecins britanniques, le docteur Greg Irving, de l'Institut de santé publique de l'université de Cambridge, et le docteur John Holden, médecin généraliste, avaient publié un article universitaire très remarqué, dans lequel ils proposaient un système de suivi de la recherche médicale fondé sur la blockchain, pour renforcer sa transparence et, *in fine*, sa crédibilité. « La confiance accordée à la recherche scientifique est diminuée par les preuves que les données ont été manipulées. Changement des résultats, sélections des seules données favorables et publications sélectives font partie des problèmes qui minent l'intégrité de la recherche publiée[18] », commentent-ils en introduction. Pour y remédier, Greg Irving a donc mis au point un protocole rapide, efficace et peu

coûteux. L'idée, vérifiée par son confrère John Holden, est d'utiliser la blockchain Bitcoin pour permettre un suivi et un audit de chaque étape d'un essai ou d'une expérience médicale. Au fil du processus, l'empreinte numérique de chaque document relatant un résultat (son hash) est inscrite et datée dans la blockchain, si bien que toute modification ultérieure du document est visible, car alors l'empreinte numérique est différente. « La méthode que nous avons décrite permet à n'importe qui de vérifier l'exacte formulation et l'existence d'un protocole à n'importe quel moment. Elle peut permettre de vérifier d'une manière fiable et automatisée que les résultats annoncés sont conformes à ceux spécifiés précédemment. Cette preuve doit pouvoir accroître la confiance et diminuer la suspicion qui entoure les données fournies et les conclusions qui en sont tirées », concluent les auteurs.

L'intérêt de la blockchain dans la santé ne se limite pas aux essais thérapeutiques. Aux États-Unis, la start-up Blockchain Health Co, basée à San Francisco, propose un système dans lequel les patients peuvent choisir de mettre leurs données de santé à disposition des chercheurs. Les premiers restent maîtres de leurs informations personnelles, en pouvant suivre l'utilisation qui en est faite, tandis que les seconds mettent la main sur un réservoir de données précieux et authentiques, pour mettre au point de nouveaux traitements, le tout dans un registre auditable par les autorités de contrôle. La gestion des données médicales est un immense marché, sur lequel le géant néerlandais Philips s'est positionné en s'associant successivement en 2015 et en 2016 à deux sociétés spécialisées, Tierion et Gem (qui, pour cette dernière, a développé une blockchain de la santé destinée à accueillir, sécuriser et rendre exploitable les données de santé, notamment par les chercheurs).

La cryptographie en guerre contre les blood diamonds

En 2007, le film hollywoodien *Blood Diamonds*, avec Leonardo DiCaprio en tête d'affiche, attirait l'attention du public sur le sinistre commerce des « diamants du sang » : ces pierres précieuses revendues illégalement par des groupes armés pour financer la guerre civile, en Sierra Leone, qui s'étala de 1991 à 2002. Les diamantaires et les gouvernements des pays producteurs et clients n'avaient pas attendu la sortie de ce long-métrage à succès pour intervenir. En mai 2000, ils se rassemblaient pour lancer le processus de Kimberley, une initiative conjointe visant à empêcher le commerce des diamants du sang. Elle a débouché sur un système international de certification des diamants, en vigueur depuis 2003 : le parcours de chaque diamant doit être retracé, de son extraction dans une mine jusqu'à son exportation, illégale sans ce certificat. En théorie. Car ce système a été vivement critiqué depuis, notamment par l'ONG Global Witness. Dans un rapport de 2010, intitulé « Le retour des diamants du sang », elle soulignait l'inefficacité du processus de Kimberley, qui se refusait à exclure le Zimbabwe, malgré la violence et la corruption qui sévissaient dans ses mines de la région de Marange, à l'Est du pays [19]. Trois ans plus tard éclatait une violente guerre civile en Centrafrique : une fois encore, le système échouait à empêcher l'exportation de diamants par des groupes armés, malgré un embargo de trois ans [*4]. C'est dans ce contexte que la Britannique Leanne Kemp, forte d'une dizaine d'années d'expérience dans le secteur du diamant et de l'assurance, a eu l'idée de monter Everledger : une blockchain dédiée à la traçabilité

des diamants. « L'industrie du diamant est très exposée aux activités criminelles[20] », écrit-elle dans le rapport publié en janvier 2016 par le UK Government Office for Science. « Les pierres sont petites et faciles à transporter et à cacher, les transactions sont souvent confidentielles et les diamants conservent leur valeur pendant de nombreuses années. C'est pourquoi ils sont utilisés dans le cadre du blanchiment d'argent et du financement du terrorisme à l'échelle mondiale. Des efforts ont été faits pour entraver cette activité illicite, notamment en traçant l'origine des diamants par un certificat papier obligatoire. Mais les contrefaçons sont très répandues […] et de nombreux pays, où le commerce du diamant représente une activité importante, ont encore une législation trop laxiste contre ces crimes. » Le registre blockchain d'Everledger offre une solution pour tracer, de manière fiable et infalsifiable, l'identité et le parcours de chaque diamant. Il constitue « une vérité unique concernant les diamants, consultable par l'industrie, les gouvernements, les consommateurs, les douanes et les polices », résume Leanne Kemp dans le rapport.

Chaque pierre se voit d'abord attribuer une sorte de passeport digital, où sont inscrits une quarantaine de points de données qui serviront à l'identifier : « Nous enregistrons son numéro de série, ce qu'on appelle ses quatre C (couleur, taille – *cut* en anglais –, pureté – *clarity* –, et poids en carats), toutes ses dimensions, ses éventuels défauts, ses inclusions[21]… », énumère Leanne Kemp. L'empreinte numérique de ces informations (le hash) est inscrite dans la blockchain. Chaque transaction relative à la pierre, de la mine à son exportation et son arrivée en bijouterie, est elle aussi renseignée dans Everledger et inscrite dans la blockchain. Pour le moment, le service d'Everledger s'adresse avant tout aux compagnies d'assurances : « Elles doivent être certaines que les diamants qu'elles assurent sont d'origine légale et veulent connaître leur valeur », précise la fondatrice. Mais les clients finaux, amateurs de bijoux ornés de diamants, bénéficieront aussi, indirectement, des améliorations offertes par ce système. Everledger collabore ainsi avec le site de vente en ligne eBay, pour l'aider à vérifier que les diamants mis aux enchères sur la plateforme proviennent bien d'une origine éthique. La société alerte également Interpol [*5] quand une transaction suspecte est repérée. Lancé en avril 2015, Everledger avait déjà réussi à constituer une base de données de près d'un million de diamants polis en août 2016, en récupérant et cryptant les informations fournies par les quatre plus grandes maisons de certification dans le monde. Un beau succès. La PDG d'Everledger ambitionne d'en enregistrer 15 millions par an. Dans un second temps, la société enregistrera également les diamants bruts.

Œuvres d'art, grands crus et sacs à main

Mais Leanne Kemp prévoit aussi de se diversifier dans un secteur inattendu, qui, sous certains aspects, ressemble beaucoup à celui du diamant : l'art. Là aussi, un système permettant d'améliorer la traçabilité des œuvres aiderait grandement à lutter contre les faussaires, le vol et le blanchiment, et séduirait les compagnies d'assurances. En mai 2016, Everledger a ainsi dévoilé un partenariat avec la société londonienne Vastari, dans laquelle elle a investi. Cette PME est spécialisée dans la mise à disposition de catalogues privés d'œuvres d'art (de musées ou de collectionneurs) aux institutions qui veulent organiser des expositions. Objectif de l'alliance : utiliser le système d'Everledger pour combattre

la fraude sur le marché de l'art. « Nous allons enregistrer les caractéristiques des œuvres d'art sur la blockchain[*6], ainsi que différents points d'inspection (des pigments de peinture par exemple). C'est assez compliqué, cela va nous prendre du temps », admet Leanne Kemp. Mais le service apporterait une vraie plus-value au secteur : « La transparence et la présence d'un historique bien documenté sur une œuvre d'art sont des facteurs cruciaux lors des prêts, des tournées d'exposition et pour les compagnies d'assurances des œuvres montrées dans les musées du monde entier. Chez Vastari, nous avons remarqué que les œuvres les plus demandées par les musées pour les expositions sont aussi celles dont l'origine et l'historique sont les mieux documentés », commentait la PDG de Vastari, Bernadine Bröcker Wieder, sur le blog de la compagnie lors de l'annonce du partenariat.

L'art n'est qu'une étape dans la stratégie d'Everlegder, qui voit grand et pense à se diversifier dans les biens de consommation de luxe, comme les sacs à main et les bijoux, et dans le vin. Trois mois plus tard, mi-novembre 2016, Maureen Downey, une sommelière américaine experte dans la détection de grands crus contrefaits, annonçait un partenariat avec Everledger pour lancer « Chai Wine Vault System », un système d'authentification digitale de bouteilles de vins de collection, dont la provenance, l'histoire et les caractéristiques (au moins 90 informations différentes) sont enregistrées de manière sécurisée dans la blockchain d'Everledger. L'inspection d'une bouteille par l'experte, suivie d'un rapport et de l'inscription des données dans la blockchain, est facturée 700 dollars et 1 200 dollars. La somme peut paraître élevée, mais le service séduira sans doute les grands collectionneurs américains, encore traumatisés par l'affaire Rudy Kurniawan : un faussaire de génie, qui avait écoulé aux États-Unis, pendant plus de dix ans, des centaines de caisses de grands crus contrefaits, pour plusieurs de dizaines de millions de dollars[*7].

---

*1. Cette société estonienne fait partie des plus anciennes et des plus grandes entreprises mondiales spécialisées dans la blockchain, avec 130 salariés et plus de 23 millions d'euros de chiffre d'affaires.

*2. Ethereum en général.

*3. Par exemple la compagnie aérienne qui achète un avion à Airbus.

*4. Levé depuis juin 2016.

*5. L'organisation internationale de la police criminelle.

*6. Titre, provenance, historique de ses expositions précédentes, taille…

*7. Arrêté en 2012 par le FBI, il a été condamné l'année suivante à dix ans de prison et à rembourser 28,5 millions de dollars aux collectionneurs qu'il avait dupés.

CHAPITRE 7

Un pilier pour la démocratie et l'administration de demain

Le 21 mars 1994, lors de l'inauguration de la première conférence mondiale des télécommunications à Buenos Aires, le vice-président des États-Unis, Al Gore, s'enthousiasmait de l'incroyable potentiel des « autoroutes de l'information », ces réseaux mondiaux de câbles qui s'apprêtaient à relier la terre entière à l'Internet naissant. À ses yeux, celles-ci allaient « promouvoir le fonctionnement de la démocratie en augmentant formidablement la participation des citoyens au processus de décisions[1] ». Audacieux, il ajoutait même : « J'y vois un nouvel âge de la démocratie athénienne. » Vingt-deux ans plus tard, le système représentatif des grandes démocraties occidentales est resté exactement le même. Internet était aussi supposé révolutionner l'administration, appelée à se réinventer au service de l'usager. En 1998, le gouvernement français de Lionel Jospin lançait son Programme d'action gouvernemental pour la société de l'information (Pagsi), qui prévoyait notamment un État « plus transparent et plus efficace », modernisé par la généralisation de l'administration électronique. Depuis, des progrès ont bien été faits : un grand nombre de démarches peuvent être réalisées en ligne (mais pas toutes). L'efficacité s'est sans doute accrue, mais la transparence fait défaut : combien de Français savent, par exemple, que l'État vend nos données personnelles ? Depuis la loi d'orientation et de programmation pour la performance de la sécurité intérieure 2 (Loppsi 2), de 2011, le ministère de l'Intérieur a le droit de monnayer les informations du fichier des cartes grises (SIV). Là encore, Internet n'a pas tenu toutes ses promesses.

C'est qu'il manquait peut-être jusqu'ici un élément pour permettre au Web d'atteindre ses fabuleux objectifs d'origine : la blockchain. Capable de fournir la transparence et la sécurité souhaitées aux services de l'administration, elle serait aussi le support idéal de systèmes de votes électroniques fiables, condition de l'avènement d'une véritable démocratie participative. Un peu partout dans le monde, des

jeunes créateurs de start-up en sont convaincus et veulent reformater, pour de bon, la représentation et l'administration publiques.

Réinventer la démocratie

En octobre 2014, sur la scène de la conférence Ted, à Rio de Janeiro, l'activiste argentine Pia Mancini faisait un constat éloquent : « Nous sommes des citoyens du XXIe siècle, qui faisons de notre mieux pour nous débrouiller avec des institutions conçues au XIXe siècle, et fondées sur une technologie du XVe siècle [l'imprimerie][2]. » Quand la plupart des grandes démocraties ont posé leurs fondations, elles ont opté pour un modèle représentatif, adapté à leur époque : tous les citoyens ne pouvant se rassembler en permanence pour s'exprimer sur chaque enjeu, leur voix étaient déléguées le temps d'un mandat à un élu, entièrement libre ensuite de voter les lois comme bon lui semblait, jusqu'à la prochaine élection. Mais ce modèle, où le citoyen ne se fait entendre qu'à chaque scrutin, est à bout de souffle. Dans l'Hexagone, selon une enquête Ipsos-Sopra Steria, publiée en novembre 2016[3], 77 % des Français estiment que la démocratie fonctionne de moins en moins bien ; 65 % d'entre eux jugent que leurs préoccupations ne sont pas prises en compte ; 62 %, qu'ils sont mal représentés ; 74 %, que les élus sont trop souvent corrompus ; et pas moins de 78 % considèrent que les partis politiques constituent la plupart du temps un frein à l'amélioration de la situation en France. Un désaveu spectaculaire pour nos représentants. Dans la plupart des grandes démocraties d'Occident, la situation n'est guère meilleure. Le système représentatif suscite aujourd'hui soit l'indifférence (qui se manifeste par des records d'abstention), soit la colère (incarnée par les succès électoraux des partis populistes).

Une stupéfiante étude américaine publiée dans la revue universitaire *Journal of Democracy* en janvier 2017 montre que l'idée même de démocratie est désormais de plus en plus rejetée par les nouvelles générations d'électeurs[4] : alors que 75 % des Américains nés en 1930 jugent essentiel le fait de vivre en démocratie, moins de 30 % de ceux nés en 1980 partagent la même opinion. Des chutes comparables de ces pourcentages sont observées au Royaume-Uni, en Nouvelle-Zélande et en Australie (elles sont un peu moindres, mais fortes tout de même, en Suède et aux Pays-Bas). Comment expliquer une telle désaffection ? Sans doute par l'inadaptation du système représentatif actuel. Aujourd'hui, Internet devrait permettre de redonner au citoyen sa voix. « Notre système politique est resté le même pendant deux cents ans et espère que nous allons nous contenter d'être les auditeurs passifs de ce monologue »,

s'offusquait Pia Mancini, sur la scène de la conférence Ted. Pourtant, soulignait-elle, « maintenant, une nouvelle technologie [Internet] nous donne la possibilité de participer à n'importe quelle conversation partout dans le monde. Nous pouvons plus que jamais exprimer nos désirs et nos inquiétudes. […] Nous voulons un siège à la table où se prennent les décisions ». C'est qu'il est grand temps de mettre en œuvre le changement promis par Internet : « Notre système politique peut être transformé, pas par la subversion ou la destruction, mais en le raccordant aux outils qu'Internet nous offre. »

Dans un premier temps, Pia Mancini a lancé une application *open source*, Democracy OS, conçue pour faire voter les élus conformément aux souhaits exprimés par les administrés. Elle a ensuite fondé, en Argentine, le Partido de la Red (parti du Net), un mouvement politique qui promettait à ses électeurs que le représentant élu voterait constamment selon les instructions transmises par ces derniers *via* l'application Democracy OS. Crédité de seulement 1 % des voix lors de l'élection du parlement local de Buenos Aires, à laquelle il s'est présenté en 2013, le Partido de la Red n'a malheureusement pas eu d'élu. Mais cette première étape encourageante a montré le chemin et marqué les esprits, et c'est avec un autre outil que Pia Mancini veut maintenant, avec ses collègues de la fondation non lucrative Democracy Earth, cofondée avec l'Argentin Santiago Siri, réinventer de fond en comble la représentation et la prise de décision politiques en démocratie : la blockchain.

Garantir la fiabilité du vote électronique

L'un des principaux objectifs de la fondation Democracy Earth est de concevoir un système de vote électronique sur le Web entièrement fiable. Car pour l'instant, le vote par Internet ou sur des machines à voter, installées dans les isoloirs, suscite une méfiance légitime, pour des raisons de sécurité : si les résultats d'un vote sont enregistrés dans un serveur, ils peuvent être hackés ou modifiés par celui qui possède ce serveur, sans aucune trace du forfait.

Le vote électronique centralisé est peu sécurisé

Le problème est ancien, mais n'a jusqu'ici toujours pas trouvé de réponse valable. En octobre 2006, alors que 90 % de la population des Pays-Bas votait dans des urnes électroniques, deux chercheurs néerlandais avaient prouvé qu'il était facile de prendre le contrôle du système et de manipuler les résultats de manière indétectable[5]. Deux ans plus tard, le pays décidait de revenir aux bulletins papier. En 2015, aux États-Unis, un rapport du Brennan Center for Justice soulignait à son tour que dans 43 États sur 50, les machines utilisées avaient plus de dix ans et étaient par conséquent très vulnérables à des pannes ou des attaques[6]. Le 4 novembre 2016, au beau milieu du scrutin présidentiel, une société de sécurité informatique, Cylance, en fournissait la preuve, prenant en quelques minutes le contrôle d'une machine « Sequoia AVC Edge Mk1 », utilisée en Californie, en Floride ou dans le New Jersey. En

France, le vote sur machine électronique est autorisé depuis 1969, mais un moratoire le limite depuis 2007 à 83 communes (1,5 million d'électeurs potentiels). Un rapport parlementaire de 2014, rédigé par les sénateurs Alain Anziani (PS) et Antoine Lefèvre (LR), pointait « l'incapacité à concilier parfaitement la technique du vote électronique avec les principes fondamentaux de la démocratie élective : la sincérité du scrutin et le secret du suffrage[7] ». Introduite dans le droit français en 2003, la consultation par Internet n'est autorisée que pour les Français de l'étranger. Elle fait elle aussi l'objet de critiques : « Les exigences constitutionnelles de sincérité et de secret du vote ne peuvent pas être aussi bien garanties par le vote par Internet que par un vote au sein d'un bureau de vote », écrivaient les sénateurs. Malgré leurs conclusions critiques et les failles avérées de ces systèmes, machines à voter et vote par Internet seront pourtant bien utilisés lors de la prochaine présidentielle française. Étonnante légèreté alors que le récent scrutin américain devrait servir d'avertissement : si aucune preuve de manipulation du vote électronique n'a été apportée, le directeur du renseignement national, James Clapper, a néanmoins publiquement pointé du doigt, dans un communiqué publié le 7 octobre 2016, l'ingérence du gouvernement russe, responsable selon lui d'avoir dirigé les attaques informatiques menées par des hackers, depuis le sol russe, sur les serveurs du parti démocrate et le compte e-mail du directeur de campagne d'Hillary Clinton, John Podesta[8]. Dans cette déclaration, il rassurait néanmoins ses concitoyens sur le vote à venir, protégé non pas par la fiabilité des machines électroniques, mais par le fait que celles-ci n'étaient pas raccordées à Internet et formaient donc un maillage décentralisé fastidieux à hacker…

Décentraliser le vote pour le sécuriser

Le vote électronique, *a fortiori* sur Internet, est-il donc condamné à rester une chimère ? Les membres de Democracy Earth ne se résignent pas, car ils ont, avec la blockchain, un nouvel atout dans leur manche. « Nous essayons de donner naissance à un système de vote électronique, par une application Web facile à utiliser et à déployer, qui permettrait à ses utilisateurs d'avoir un suivi de leur vote[*1], tout en empêchant les organisateurs du scrutin de modifier ses résultats et d'avoir accès aux informations personnelles des votants », résume Louis Margot-Duclot, porte-parole en France de la fondation. Pour cela, la plateforme s'appuiera sur la technologie blockchain, qui garantit l'enregistrement décentralisé de chaque vote au sein des ordinateurs du réseau (comme une transaction Bitcoin). Impossible donc de changer le résultat après coup. L'identification de chaque votant, élément essentiel à la fiabilité du scrutin, sera également faite sur la blockchain (bien que peu d'informations soient encore apportées sur ce point). Grâce à la blockchain, Democracy Earth comblera les failles relevées par le projet dont il est héritier, DemocracyOS : « Democracy OS permet à n'importe qui de proposer sur Internet, auprès d'une instance de décision collaborative, des textes, sur lesquels on peut voter en commentant notre décision », rappelle Louis Margot-Duclot. « L'avantage était la simplicité de sa mise en place, mais la plateforme qui a accès à la base de données accède aussi au résultat du vote, et peut lui faire dire ce qu'elle veut. Ça pose un problème de confiance », admet-il. Ce ne sera plus le cas avec la plateforme blockchain développée par Democracy Earth. « Nous donnerons à l'organisateur d'une consultation collective la

capacité de prouver que le résultat final de la délibération est intact, et représente fidèlement le résultat », promet Louis Margot-Duclot.

Un prototype a été testé à l'automne 2016. Un scrutin en ligne, de portée symbolique, a été organisé par Democracy Earth en parallèle du référendum mené en Colombie sur la réconciliation avec les Farcs[*2], pour permettre aux Colombiens vivant hors du pays de voter. Le résultat a été surprenant : 83 % des votants électroniques se sont exprimés pour la réconciliation avec les Farcs, alors que les Colombiens restés au pays ont rejeté l'accord de paix à 50,2 %. « Cela nous a permis de réaliser les premières élections sur la blockchain Bitcoin », se réjouit l'expert français. Les participants n'avaient pas besoin d'acheter de Bitcoin ni de payer quoi que ce soit pour voter : chaque suffrage était enregistré comme une microtransaction dont le coût, négligeable, était pris en charge par la fondation. Une première expérience prometteuse.

L'enjeu de l'identification du votant

Parallèlement à Democracy Earth, d'autres start-up mènent des initiatives similaires, comme l'américaine Follow My Vote ou la PME française Belem, créée en novembre 2015. Celle-ci a développé un module de vote en ligne sur la blockchain Ethereum, auditable par tous : chacun peut constater l'issue du vote et vérifier qu'elle correspond bien à l'ensemble des suffrages exprimés, consultables dans des transactions publiques sous pseudonymes notés sur le registre. L'entreprise vise toutes les élections, aussi bien professionnelles (comité d'entreprise, représentant du personnel) que politiques (scrutin et référendums en tout genre), économiques ou associatives (assemblées générales, votes de sociétaires de mutuelles, copropriété, etc.). Le géant de la construction, des parkings et des autoroutes, Vinci, a déjà adopté la solution de Belem. C'est aussi le cas du mouvement Nous Citoyens, lancé en juillet 2013 par l'entrepreneur Denis Payre, et qui a testé le module de Belem lors de ses élections internes régionales et départementales, en avril 2016. L'expérience a plutôt réussi. « Nous avons pu confirmer l'efficacité du vote blockchain. C'est une innovation technologique indéniable car elle permet d'organiser une élection fiable et transparente, une optimisation nette du vote digital tel qu'il était pratiqué jusque-là[9] », se réjouissent les fondateurs de Belem, Côme Jean Jarry et Romain Rouphael. Mais ils concèdent toutefois avoir constaté deux limites à leur solution : « Voter *via* la blockchain ne peut pour l'instant se substituer intégralement au vote physique, seul système à ce jour capable de véritablement certifier l'identité du votant et de garantir le secret de l'isoloir. Nous n'avons pas encore les moyens techniques nécessaires à la vérification de l'identité du votant : rien ne peut aujourd'hui contrer le piratage de la boîte mail, l'usurpation d'identité ou les jeux d'influence », écrivent-ils. Autre inconvénient observé : la validation de chaque transaction, qui prend quelques minutes, ce qui obligerait à organiser un vote sur plusieurs jours dans le cas d'une élection à très grande échelle. Mais rien d'insurmontable *a priori* : aux États-Unis par exemple, l'élection présidentielle s'étale sur plusieurs semaines.

La véritable difficulté, encore une fois, réside dans l'identification du votant. « Nous pouvons imaginer que dans un futur proche, l'exercice de vote en ligne soit associé à un capteur biométrique qui permettrait à l'électeur de s'identifier de façon fiable et ainsi d'assurer la validité de son identité », suggèrent Côme Jean Jarry et Romain Rouphael. Mais les électeurs accepteraient-ils que leur vote, une fois déposé, reste lié à leur identité ? Que deviendra l'anonymat de chaque suffrage ? En Estonie, pays balte très en avance sur le reste du monde dans l'utilisation administrative des nouvelles technologies, le vote électronique par Internet est déjà possible depuis 2005. C'était alors une première mondiale. Les électeurs s'identifient devant leur ordinateur en insérant leur carte d'identité, qui contient une puce électronique. Mais leur système, qui n'utilise pas la blockchain, fait encore débat. « À chaque fois que le parti conservateur perd, ils disent que c'est la faute du vote électronique, et contestent sa fiabilité[10], bien qu'aucune fraude n'ait jamais été mise au jour dans les neuf scrutins électroniques que nous avons organisés jusqu'ici », regrette Anna Piperal, la directrice du *showroom* e-Estonia, l'organisme qui promeut les services numériques du pays. Le pays pourrait faire appel à la blockchain pour mettre fin, pour de bon, à toute suspicion sur la validité des scrutins. La start-up estonienne Guardtime, l'une des plus anciennes et des plus grosses sociétés mondiales dans le secteur des registres distribués, a proposé d'intégrer la blockchain au système de vote électronique. « Ce système rendrait impossible toute manipulation des résultats », insiste Anna Piperal. « Leur solution permettrait en plus de conserver l'anonymat du vote tout en offrant aux électeurs la possibilité de vérifier que leur voix a bien été attribuée au candidat de leur choix », ajoute-t-elle.

Débattu mais pas mis en place pour le moment, ce projet manque de volonté politique pour être appliqué. En France, même les élus les plus ouverts à la blockchain, comme le député LR de Haute-Savoie, Lionel Tardy, veulent rester prudents avant de se lancer dans de telles aventures : « Je suis très méfiant sur le vote électronique pour des questions de sécurité. La blockchain pourrait aider. On pourrait faire des étapes, par exemple une procuration électorale par la blockchain. Cela pourrait répondre à la crise de confiance vis-à-vis du politique et faire baisser l'abstention[11] », a-t-il déclaré lors du Forum parlementaire de la blockchain. À l'automne 2016, l'association LaPrimaire.org, qui organisait une primaire en ligne pour faire élire un candidat citoyen à la présidentielle 2017, s'est lancée. « Nous avons organisé l'un des premiers scrutins numériques au monde sur la blockchain[12] », se félicite le fondateur, David Guez. Au premier tour, plus de 12 000 personnes ont participé. Les votes étaient enregistrés sur la blockchain Ethereum. Malgré cette première encourageante, la France attendra sans doute de voir le vote électronique sur la blockchain appliqué avec succès par une autre grande démocratie avant de se lancer. L'Australie est candidate à l'expérience. À l'été 2016, la Poste locale, Australia Post, s'est ainsi proposée pour devenir organisatrice d'élections sur la blockchain, d'abord pour des scrutins d'entreprises et de communautés, avant de passer, dans un second temps, aux élections parlementaires. Le système annoncé est très similaire à ceux de Belem ou de Democracy Earth : les votes seraient enregistrés comme des transactions électroniques, sécurisées par des clés privées envoyées à chaque votant, dont la voix serait anonymisée une fois déposée[13]. À suivre.

Démocratie liquide

Si la blockchain permet enfin un mécanisme fiable de vote électronique sur Internet, alors c'est tout le fonctionnement démocratique qui peut être rénové de fond en comble. Un tel système pourrait contribuer à faire baisser l'abstention, en facilitant la vie des électeurs éloignés des bureaux de vote (et des paresseux). En Estonie, où presque un tiers de la population a désormais pris l'habitude de voter sur Internet, la participation aux élections locales a augmenté de 10 points entre 2005, date du premier vote électronique, et 2013 (47,4 % contre 58 %[14]) et de 2 points aux élections parlementaires entre 2007 et 2015 (61,9 % et 64,2 %). L'effet est toutefois à nuancer, car les élections européennes, par exemple, n'ont pas mobilisé les Estoniens, malgré la possibilité de voter en ligne (36,5 % de participation en 2014, contre 43,9 % en 2009).

Mais il s'agit là encore de formes de vote classique, dupliquées sur Internet. D'autres types de consultation et d'expression des votants peuvent être imaginés, pour faire émerger une nouvelle forme de démocratie, plus fidèle aux aspirations des citoyens : la « démocratie liquide ». Cette expression un peu obscure désigne tous les systèmes, aux configurations innombrables, de délégation et de subdivision du vote : pour un vote donné, vous pouvez choisir de transmettre votre voix à la personne de votre choix, ou d'en conserver la moitié et de lui confier l'autre, ou encore de céder n'importe quelle proportion de votre bulletin à n'importe quel nombre de votants. Vous pouvez aussi retirer votre voix au candidat en cours de mandat s'il n'agit plus conformément à vos convictions, ou encore choisir de pondérer votre voix sur les thèmes qui vous sont chers : 40 % de votre bulletin sur l'économie, 40 % sur la sécurité, 20 % sur l'éducation par exemple. Cela demande alors de réimaginer des scrutins non plus sur des candidats mais sur des plateformes de propositions. Les possibilités sont infinies et rebattent complètement les cartes des élections telles que nous les connaissons, avec un objectif : apporter une plus grande précision et une meilleure fidélité à la représentation politique, et laisser au votant un contrôle supérieur sur son représentant. « La démocratie représentative telle qu'on la connaît aujourd'hui, c'est voter tous les cinq ans, pour un candidat, qui va porter un programme de mesures. Ces trois éléments changent dans la démocratie liquide », souligne Louis Margot-Duclot. Plus de mandat d'abord, puisque la voix peut être retirée à n'importe quel moment. Plus d'hommes politiques de profession non plus, obligés d'être omniscients sur tous les sujets de débat : la voix peut être déléguée à des experts sur chaque sujet, ou distribuée à différentes idées plutôt qu'à un homme. « Si on a un ami qui connaît bien l'économie, à laquelle on ne comprend rien, et que l'on est d'accord avec lui, on va pouvoir lui déléguer son vote, puis lui-même va pouvoir déléguer son vote, jusqu'à ce qu'on arrive à un candidat ou une disposition spécifique », illustre Louis Margot-Duclot. « On passe d'un choix binaire qui porte sur des personnes et sur une période fixe dans le temps à un modèle où l'on peut voter mesure par mesure, en fonction des sujets que l'on délègue ou non. En un mot, on va préciser la quantité d'information contenue dans un vote et raffiner ainsi la représentation politique, qui est aujourd'hui à bien des égards trop vaste et a perdu le lien direct avec les électeurs », résume-t-il. Un tel système permettrait peut-être de remobiliser le corps électoral : « Si je suis à moitié d'accord avec un candidat, je vais avoir à moitié envie d'aller voter. Là,

vous allez pouvoir voter mesure par mesure, ce qui permet d'obtenir un panel beaucoup plus représentatif des désirs des électeurs », insiste-t-il. Sa fondation, Democracy Earth, travaille actuellement au développement d'une plateforme de vote de ce type, avec pour ambition l'émergence d'une véritable démocratie pair à pair, dont les représentants seraient issus de la volonté populaire et ne lui auraient été pas imposés par des partis.

Repenser les services de l'État

En janvier 2016, le Government Office for Science, l'organisme de conseil scientifique du gouvernement britannique, publiait un long rapport précurseur sur les possibilités offertes par la blockchain pour l'économie et l'État. Les auteurs y listaient notamment les innombrables applications possibles de cette technologie pour améliorer l'action publique : « Les registres distribués peuvent aider les gouvernements à collecter les taxes, distribuer les allocations, émettre des passeports, enregistrer des titres de propriété, assurer l'approvisionnement de biens et plus généralement garantir l'intégrité des fichiers et services du gouvernement. Pour la Sécurité sociale[*3], cette technologie permet de faire progresser les soins en améliorant et en authentifiant les services dispensés et en partageant des fichiers de manière sûre selon des règles précises. Pour les bénéficiaires de ces services, cette technologie permet, selon les circonstances, de contrôler l'accès à ses données personnelles et de savoir qui les a consultées[15]. » Décentralisées dans un réseau de multiples ordinateurs, les données sont aussi plus difficiles à hacker ou à truquer, ajoutent les auteurs. « En résumé, la technologie des registres distribués fournit au gouvernement une structure pour réduire la fraude, la corruption, le risque d'erreur et le coût de procédures auparavant réalisées sur papier. Elle a le potentiel de redéfinir la relation entre le gouvernement et le citoyen en matière de partage des données, de transparence et de confiance. » Fabuleux programme ! Il n'a pourtant rien d'utopique, comme le prouve le cas de l'Estonie, où l'administration numérique sur la blockchain est d'ores et déjà la règle.

L'ADMINISTRATION ESTONIENNE, 100 % ÉLECTRONIQUE ET 100 % TRANSPARENTE

Le 20 août 1991, l'Estonie, la plus au nord des trois républiques baltes, arrachait son indépendance à l'Union soviétique. L'économie est alors dans un état de grand délabrement et toute l'administration doit être refondée de A à Z. Cet incroyable défi est finalement la chance du pays, qui l'a saisie pour

devenir aujourd'hui la nation la plus numérisée de la planète. Son premier gouvernement, dirigé par une équipe de trentenaires libéraux emmenés par le jeune Mart Laar, 32 ans, lance un vaste programme de réformes pour ouvrir son économie sur le monde et pose les bases d'une nouvelle administration qui deviendra largement dématérialisée. « Nous étions dans une situation où il nous fallait bâtir un nouveau capitalisme, pour lequel il n'existait pas de structure légale. L'Estonie avait des informaticiens très qualifiés et nous avons pu partir de zéro. La moitié du territoire est couvert de forêts, c'était difficile d'installer des bureaux pour l'administration dans tout le pays. C'est pourquoi, pour des raisons financières, tant de procédures ont été numérisées. Nous avons essayé de construire un service public efficace sans contact physique[16] », explique Anna Piperal.

La construction de cette administration 100 % numérique s'est faite en trois temps. En 2002, l'État a émis une carte d'identité électronique, utilisée aujourd'hui par 94 % de la population. Ce document d'identité est équipé d'une puce qui contient des clés cryptographiques permettant à son possesseur de s'identifier pour accéder à l'ensemble des services administratifs en ligne, pour voter, mais aussi pour acheter un ticket de transport ou pour récupérer une prescription à la pharmacie. La seconde étape a été l'interconnexion progressive, grâce à l'entrée commune offerte par cette carte d'identité numérique, de toutes les bases de données numériques des différents services de l'État. Cette réforme, lancée dès 2001, a donné naissance au système « *X road* » (« carrefour » en français) : l'intersection de 170 bases de données publiques, offrant plus de 2 000 services à plus de 900 organisations (institutions, ministères et entreprises privées). « La loi oblige les institutions gouvernementales à échanger les informations dont elles disposent. Cet échange a lieu par le protocole cryptographique *X road*. Ainsi, quand je m'enregistre sur le site des impôts, par exemple, ma déclaration est préremplie avec les informations de mon employeur, et la banque vérifie automatiquement que ces informations sont correctes sans que le gouvernement ne sache combien j'ai sur mon compte », illustre Anna Piperal. Grâce à cette interconnexion complète des services de l'administration, tout peut être fait facilement en ligne : la demande d'un certificat de résidence, la déclaration fiscale, le renouvellement du permis de conduire, l'assurance automatique d'un nouveau-né, la création d'une entreprise, etc.

Mais toutes ces données sont fragiles : comment garantir que personne ne les consulte indûment ? Qu'elles n'ont pas été modifiées ou volées ? C'est là qu'intervient la blockchain. En 2007, la question de la sécurité de ce trésor de données personnelles s'est posée avec acuité, alors que le pays était victime d'une attaque informatique sans précédent. Fin avril 2007, le gouvernement décide d'enlever d'un parc de la capitale, Tallinn, la statue de bronze d'un soldat soviétique, pour la déplacer dans un cimetière militaire. La décision est vécue comme un affront par la Russie. Dans ce contexte, des pirates mènent, depuis le sol estonien et le sol russe, une campagne d'attaques informatiques massives contre quasiment toutes les institutions du pays : le parlement, les banques, les médias et les partis politiques. *A priori*, aucune donnée n'est dérobée, mais les sites et services connectés tombent les uns après les autres. Les Estoniens ne pouvaient par exemple plus tirer d'argent. « Ça a fait réfléchir le gouvernement, qui a réalisé que l'Estonie reposait beaucoup sur son infrastructure digitale de e-gouvernement. Certains pensaient que ces attaques avaient des motivations politiques et que des gens, au sein même de notre

système d'information, pouvaient ne pas être loyaux envers l'Estonie, et agir sans que personne ne s'en rende compte[17] », raconte Martin Ruubel, responsable des opérations de e-gouvernement chez Guardtime. « Or si vous êtes à l'intérieur d'un système, vous pouvez faire ce que vous voulez, comme Edward Snowden l'a prouvé », insiste-t-il.

À la demande du gouvernement, Guardtime installe donc, en avril 2008, une infrastructure cryptographique équivalente à la blockchain, même si elle n'en portait pas à l'époque le nom. Baptisé KSI (Keyless Signature Infrastructure), ce registre public distribué (comme la blockchain Bitcoin) permet de vérifier, de manière indépendante, si une donnée a été consultée ou changée, par l'inscription de son hash unique dans la blockchain. Ce système assure, encore aujourd'hui, l'intégrité des données. « Si un médecin essaie de consulter mon dossier médical par exemple, cela laissera une trace et j'en serai avertie. S'il le fait sans mon autorisation, je pourrai porter plainte et il risquera de perdre sa licence », illustre Anna Piperal. Ainsi, « personne ne peut regarder ou changer une information sans que cela ne soit vu », ajoute-t-elle. Une garantie pour les citoyens comme pour l'État : « En Estonie, il ne pourrait pas y avoir d'affaire Snowden », assure-t-elle. Toutes les bases de données publiques estoniennes ne sont pas encore raccordées à la blockchain de Guardtime, mais c'est déjà le cas de 70 % des dossiers médicaux, ainsi que des données du ministère de la Défense, des statistiques démographiques, des lois, des procédures pénales et de tous les documents relatifs aux successions. Autant d'informations pour lesquelles il est indispensable d'avoir la certitude qu'elles sont fiables et authentiques. « Dans le cas d'un héritage, c'est essentiel d'être sûr que l'information que vous donnez dans un testament sera toujours consultable et inchangée quand on en aura besoin, peut-être cinquante ans plus tard », insiste Martin Ruubel. Pour s'en assurer, l'Estonie veut aller plus encore dans la sécurisation des données de ses citoyens. Les serveurs, qui abritent les différentes bases de données reliées par *X road* et protégées par Guardtime, sont pour l'instant tous encore localisés dans le pays. « Nous devons éliminer cette faiblesse », affirme Anna Piperal. « Les données seront stockées dans les ambassades d'Estonie un peu partout dans le monde. Ainsi, si notre pays était bombardé, elles seraient toujours disponibles et en sécurité », précise-t-elle.

Un modèle pour le reste du monde

Incroyablement précurseur, pragmatique et efficace, le système d'administration électronique estonien fait des envieux partout dans le monde. La numérisation de tous ses services lui ferait économiser 2 % de PIB par an, selon les chiffres officiels[18]. Une performance qui ferait rêver plus d'un ministre du Budget en Europe. À Tallinn, le *showroom* e-Estonia, qui détaille aux visiteurs les recettes de ce miracle administratif, ne désemplit pas : « Nous accueillons 10 000 personnes par an : politiques, investisseurs, journalistes, entrepreneurs », précise Anna Piperal. La Finlande est en train d'adopter le même système de e-gouvernement. « Nous travaillons également avec le Sri Lanka et la Malaisie sur le e-gouvernement, et certaines entités du gouvernement américain nous ont contactés pour comprendre

comment nous travaillons », se réjouit Martin Ruubel. « Le Canada aimerait aussi s'inspirer de nous », ajoute Anna Piperal.

La France se lancera-t-elle un jour ? « C'est plus facile pour les pays qui n'ont pas un long héritage administratif et qui peuvent commencer de zéro », admet Martin Ruubel. « Dans certains pays, il y a aussi un manque de volonté politique : tout le monde n'est pas prêt pour autant de transparence », regrette sa compatriote. Dans l'Hexagone, certains députés, tels Laure de La Raudière (LR), poussent dans ce sens : « Le pays le plus agile aujourd'hui en Europe, c'est l'Estonie. Notre boulot, c'est de convaincre nos partenaires européens de nous mettre derrière l'Estonie, et d'en faire le porte-étendard de cette révolution technologique[19] », a-t-elle déclaré au Forum parlementaire de la blockchain. Les Français y sont ouverts : selon un récent sondage Ipsos, 88 % des personnes interrogées se déclaraient prêtes à utiliser les services en ligne proposés par l'administration[20]. Nos voisins européens se lancent timidement. Au Royaume-Uni, le rapport du Government Office for Science préconisait des expérimentations de la blockchain à court terme, par des collectivités pionnières et des services publics. En Suisse, en avril 2016, la mairie de Zoug, à 35 km au sud de Zurich, est devenue la première au monde à accepter les paiements en Bitcoin pour ses services municipaux (certificats de naissance, acte de décès, etc.). « Nous voulions voir comment cela marchait et donner aux entreprises du secteur de la blockchain un signal positif de bienvenue[21] », commente le directeur des services municipaux, Martin Würmli. Très médiatisée, cette décision est surtout une bonne opération de communication pour la ville, qui veut devenir la capitale de la « cryptovalley », une Silicon Valley des cryptomonnaies. En réalité, seulement une dizaine d'administrés ont réglé la mairie en Bitcoins dans les six mois qui ont suivi la mise en place du service. Des premiers pas encore bien loin du système d'administration 100 % numérique, sécurisé par la blockchain, que l'Estonie a su mettre en place.

Une autre application possible : lutter contre la fraude fiscale et sociale

Le modèle estonien est l'incarnation de la possibilité, offerte par la blockchain, de gérer la puissance publique de manière sécurisée et transparente. Mais cette même transparence peut aussi s'appliquer, grâce à la blockchain, à ceux qui bénéficient des services de l'État, en recevant des allocations ou des subventions, ou les financent, comme les particuliers et entreprises qui paient des impôts et des cotisations. La blockchain donne en effet la possibilité de mieux lutter contre la fraude fiscale ou sociale et de superviser au plus près la distribution de l'argent public, comme le souligne le rapport du Government Office for Science. Pour ses auteurs, « les nouveaux modèles de paiement permettront au Trésor public et au Département du travail et des pensions [responsable de la distribution des allocations retraite et familiales] de distribuer le soutien de l'État providence plus efficacement[22] ». Ce qui vaut à l'intérieur du pays vaut aussi hors des frontières : « La technologie des registres distribués permettra au gouvernement de mieux contrôler la distribution de l'aide au développement, afin de

s’assurer que les fonds sont bien reversés à ceux visés. » Enfin, la blockchain pourrait même, selon eux, sécuriser la collecte de la TVA à l’échelle européenne : « Le manque à gagner annuel de l’Union européenne sur la collecte de la TVA est estimé entre 151 et 193 milliards d’euros. […] Le développement de niveaux standard de TVA applicables dans toute l’Union européenne et de protocoles communs permettrait le déploiement d’un registre distribué dans toute l’Europe, qui ajusterait unilatéralement toutes les transactions comprenant de la TVA, des factures jusqu’aux reçus bancaires. » L’idée est bonne, mais ne sera pas mise en œuvre par des fonctionnaires britanniques puisque, 6 mois après la parution du rapport, les citoyens anglais ont opté pour la sortie de l’Union européenne. Elle reste néanmoins applicable par les autres États membres.

Plusieurs autres rapports d’experts soulignent l’intérêt d’une collecte de taxe enregistrée sur la blockchain pour minimiser la fraude. « Une blockchain dotée d’un historique complet des revenus et des transactions de vente pourrait permettre l’automatisation de la collecte de taxe, la réduction de la fraude et des formalités administratives[23] », considèrent ainsi les analystes de l’agence Moody’s. L’idée n’est pas utopique : selon une étude du World Economic Forum de 2015, la première collecte de taxe par la blockchain devrait avoir lieu d’ici six ans, en 2023. Pas moins de 73,1 % des 800 experts interrogés pour ce rapport s’accordent pour dire que cette grande première se produira en tout cas avant 2025[24].

En attendant, de grandes entreprises travaillent activement à des utilisations de la blockchain en matière de lutte contre la fraude sociale. « Dans le domaine de la santé, il y a pas mal d’optimisations possibles. La fraude, c’est une sorte d’incohérence entre ma version de la vérité et celle d’un autre. En permettant de partager les informations sur la vérité d’une transaction, la blockchain peut ramener une cohérence entre les versions de différentes personnes. Si les pharmacies, la sécurité sociale et les médecins avaient la même vision de la vérité, on réduirait largement l’impact de la fraude. Je ne peux pas en dire plus, mais ce sont des idées auxquelles nous réfléchissons », confirme Luca Comparini, d’IBM France. La start-up américaine Bithealth développe une solution de ce type, qui permettrait l’enregistrement sécurisé sur la blockchain Bitcoin de données de santé, à l’échelle mondiale.

Un cyberoffice notarial

« Vous voyez un homme gros et court, bien portant, vêtu de noir, sûr de lui, presque toujours empesé, doctoral, important surtout ! Son masque bouffi d'une niaiserie papelarde qui d'abord jouée, a fini par rentrer sous l'épiderme, offre l'immobilité du diplomate, mais sans la finesse, et vous allez savoir pourquoi. Vous admirez surtout un certain crâne couleur beurre frais qui accuse de longs travaux, de l'ennui, des débats intérieurs, les orages de la jeunesse et l'absence de toute passion. Vous dites : Ce monsieur ressemble extraordinairement à un notaire[25]. » Ces cruelles lignes de Balzac décrivent, par la caricature, une antique profession, apparue sous l'Empire romain, et que beaucoup pensaient immortelle. Pourtant, après plus de deux mille années d'existence, les notaires ont peut-être trouvé, dans la technologie blockchain, un concurrent de poids, capable de remettre en cause leur avantageuse situation. Quel est le rôle d'un notaire ? Professions libérales, mais investis d'une délégation de puissance publique, les notaires ont pour mission, selon la loi, de « recevoir tous les actes et contrats auxquels les parties doivent ou veulent faire donner le caractère d'authenticité attaché aux actes de l'autorité publique », ainsi que d'en « assurer la date », d'en « conserver le dépôt » et d'en « délivrer des grosses et expéditions »[26] (c'est-à-dire des copies). En d'autres termes, les notaires authentifient les actes, de propriété par exemple, et les contrats. Ils leur donnent une date de signature, en conservent l'original et peuvent fournir une copie à qui de droit. Mais tout cela pourrait désormais être fait sans eux, parient de très nombreuses start-up, comme l'américaine Tieron ou les françaises Keeex et Bitproof, qui se sont lancées sur le créneau de la « notarisation » de documents : l'enregistrement horodaté de l'empreinte unique d'un document dans la blockchain, qui permet de vérifier, ultérieurement, son caractère original et intact. Leur fonctionnement est très simple, comme le résume le jeune Louison Dumont, 19 ans, fondateur de Bitproof : « C'est un notaire décentralisé. Vous avez un document et vous voulez prouver qu'il existe et qu'il vous appartient. Vous nous l'envoyez, on met l'ADN de ce document dans la blockchain (le hash), et vous avez maintenant une preuve que ce document existait à une date donnée, et que vous en étiez le propriétaire[27]. » L'application, disponible sur bitproof.io, est opérationnelle et gratuite. Le 25 septembre 2016, à 20 h 08, j'y ai enregistré le précieux plan de cet ouvrage. Il a suffi de prendre un fichier sur le

bureau et de le charger sur le site, d'enregistrer une vidéo, dans laquelle j'ai répété une phrase indiquée par Bitproof : « My name is Stéphane Loignon and I'm signing the contract number 99b7-bacb-f158-7e45[*4]. » L'ADN du fichier a alors été noté dans la blockchain Bitcoin. En retournant sur le site, je peux prouver que j'ai bien déposé ce document à la date annoncée, comme en atteste le certificat de propriété téléchargeable, correspondant à la transaction passée sur la blockchain. Ainsi, si quelqu'un prétend aujourd'hui que ce document n'est pas le mien, je pourrai prouver que j'en étais déjà le possesseur à cette date.

Sur ce principe, deux premiers créneaux ont été visés à ce jour : l'enregistrement d'actes de propriété foncière (en concurrence frontale avec la profession de notaire) et celui de diplômes (un domaine non notarié, mais où la question de l'authenticité se pose également avec acuité). Mais bien d'autres peuvent être imaginés, des certificats d'assurance à l'enregistrement de contrats en passant par le dépôt d'inventions ou la protection d'œuvres d'auteur.

La blockchain à l'assaut du cadastre

Dans un essai publié en 2000, intitulé *Le Mystère du capital* et sous-titré *Pourquoi le capitalisme triomphe à l'Ouest et échoue partout ailleurs*, l'économiste péruvien Hernando de Soto avançait une explication alors inédite au sous-développement persistant d'une large partie de la planète. Selon lui, les citoyens des pays les plus pauvres sont pénalisés par l'absence de système fiable pour garantir leur droit de propriété. Beaucoup possèdent, dans les faits, une maison, un terrain, un champ, un troupeau ou une petite entreprise. Mais ils n'ont, pour aucun de ces actifs, les titres de propriété correspondant. Or, sans ces documents, impossible de vendre ou de transmettre tout ou partie de ces biens, de les louer ou de les faire fructifier : le faible capital des plus pauvres est donc « mort », selon l'expression de l'économiste. Ils sont condamnés à rester hors du vaste marché capitaliste et ne peuvent pas profiter de sa croissance. En 2000, l'économiste évaluait le montant total de ce « capital mort » à 9 300 milliards de dollars…

Une quinzaine d'années plus tard, la blockchain a remis cette théorie sur le devant de la scène, en offrant une solution simple et peu coûteuse pour résoudre le problème mis en avant par Hernando de Soto. Dans quatre pays déjà (la Géorgie, le Ghana, le Honduras et la Suède), des start-up utilisent la blockchain pour enregistrer des titres de propriété immobilière, en s'inspirant directement des idées de l'expert péruvien. En avril dernier, Hernando de Soto lui-même a annoncé un partenariat entre le ministère de la Justice de Géorgie et la compagnie californienne BitFury, chargée de concevoir et de piloter un tel programme sur la blockchain. « Pourquoi la blockchain ? Elle va nous aider à faire trois choses[28] », a déclaré Valery Vavilov, le président de BitFury, cité par le magazine *Forbes*. « D'abord, elle va sécuriser les données afin qu'elles ne puissent pas être corrompues. Ensuite, des audits publics pourront être faits en temps réel. […] Troisièmement, cela va réduire les frictions et le coût d'enregistrement des droits de propriété, car les gens pourront le faire avec leur smartphone. La blockchain sera utilisée comme un service de notaire », a-t-il indiqué. Avec un tel système, chacun peut facilement et à peu de

frais authentifier ses propriétés sur la blockchain. L'enregistrement d'un acte de vente d'un bien immobilier peut se faire à distance, avec un smartphone, pour un coût de transaction compris entre 5 et 10 centimes de dollars, contre 50 à 200 dollars auparavant, précise l'article de *Forbes*. Le rêve d'Hernando de Soto devient réalité : « Ce projet important va montrer que les gouvernements qui transfèrent leurs registres cadastraux sur une blockchain peuvent établir un système plus transparent et bien enregistré, qui bénéficiera finalement aux gens et offrira des opportunités économiques à tous[29] », s'est réjoui l'économiste.

Un projet précurseur du même type est mené au Ghana par l'ONG Bitland. « Le fondateur, Narigamba Mwinsuubo, l'a lancé en 2014 en voulant appliquer les idées d'Hernando de Soto[30] », précise l'Américain Chris Bates, *chief security officer* (directeur de la sécurité) de Bitland. Au Ghana, près de 78 % des biens immobiliers ne sont pas enregistrés officiellement. Tout est à faire. En collaboration avec le gouvernement ghanéen et avec vingt-huit communautés locales dans la métropole de Kumasi, Bitland crée donc, petit à petit, un cadastre sur la blockchain Bitcoin. Après deux années de préparation et de test, un bureau a été ouvert pour démarrer le service, en octobre 2016. « Nous enregistrons le nom du propriétaire, les caractéristiques du terrain [coordonnées GPS, description écrite, vue satellite notamment], la durée pour lequel il est possédé – car au Ghana, c'est pour 99 ans au maximum –, et nous notons si le bien fait l'objet de disputes », indique Chris Bates. Les informations sont validées par le gouvernement et les chefs locaux des communautés. Tout le monde est gagnant. Les citoyens ont enfin la preuve qu'ils sont bien propriétaires de leurs biens, ce qui leur permet de se défendre en cas de litige, de vendre, de louer ou encore d'emprunter auprès d'une banque. Le gouvernement, lui, a une vision plus claire du cadastre, ce qui lui permet de lever des taxes. Après ce premier essai pilote au Ghana, Bitland veut étendre son programme au Nigeria et ouvrir un centre à Lagos début 2017 : « Il y a là-bas le même problème d'enregistrement des titres de propriété immobilière », relève Chris Bates. Au Honduras, l'entreprise texane Factom s'est lancée dans une aventure similaire. Ce pays de 8 millions d'habitants, l'un des plus pauvres d'Amérique du Sud, souffre d'un cadastre très incomplet (60 % des biens immobiliers n'y seraient pas enregistrés), auquel s'ajoute un problème latent de corruption. « Dans le passé, le Honduras a dû faire face à des cas de fraude à la propriété foncière. La base de données du pays a été hackée. Des bureaucrates pouvaient y entrer et s'attribuer la propriété de magnifiques demeures au bord de l'eau[31] », a déclaré le président de Factom, Peter Kirby, en mai 2015 à l'agence Reuters, lors de l'annonce du lancement de ce projet d'enregistrement du cadastre sur la blockchain Bitcoin. L'entreprise espérait mettre en ligne un système pilote dès la fin 2015. En vain. Un prototype a bien été conçu pour La Ceiba, la quatrième ville du pays. Mais depuis, le programme patine. « Cela avance, mais lentement. Il est normal que de tels projets composent avec les délais de la bureaucratie, c'est l'Amérique du Sud[32] ! » justifie Abhi Dobhal, vice-président en charge du développement commercial chez Factom.

Les pays en développement ne sont pas les seuls à trouver des avantages à l'inscription du cadastre sur la blockchain. Pour preuve, la Suède a annoncé sa volonté d'expérimenter l'idée, en juin 2016. L'organisme national chargé de la propriété foncière, Lantmäteriet, a conçu, avec la start-up ChromaWay, le cabinet de conseil Kairos Future et le groupe de télécoms Telia, un prototype d'application blockchain,

capable d'enregistrer les titres de propriété issus des nouvelles acquisitions immobilières dans le pays. L'objectif est de réduire le risque d'erreur de saisie manuelle et de créer une procédure sécurisée de transfert de documents. Dès l'accord initial entre le vendeur et l'acheteur, toute la procédure d'achat, jusqu'à sa finalisation, deviendrait ainsi transparente et consultable par les deux parties concernées, mais aussi les banques ou les autorités publiques.

Remise de diplômes sur la blockchain

En 2013, *L'Express* révélait que le grand rabbin de France, Gilles Bernheim, n'était pas agrégé de philosophie, contrairement à ce qu'il prétendait. L'année précédente, le DG de Yahoo s'était fait épingler après avoir, lui aussi, gonflé abusivement son CV. Les cas sont légion. Selon une étude publiée en 2013 par le cabinet de recrutement Florian Mantione, en France, 33 % des candidats s'attribueraient de faux diplômes[33]. Un chiffre comparable au Royaume-Uni, où l'organisme officiel dédié à la vérification des diplômes[*5], créé en 2011, estime que 30 % des candidats à un poste embellissent ou exagèrent leurs parcours académiques. Les employeurs vérifient rarement, ou se contentent de demander à l'embauche une copie du diplôme, ainsi falsifiable. Il suffit de taper « *fake French diploma* » sur Google pour tomber sur une liste de sites (illégaux), recelant des contrefaçons personnalisables : licence, master, baccalauréat, brevet de technicien supérieur… Tout y est ! Pour faire face à ce fléau, le ministère de l'Éducation nationale, a annoncé, le 21 janvier 2016, la création d'attestations numériques pour les diplômes d'État délivrés en 2017, avec une rétroactivité progressive sur les quinze dernières années. Un an plus tard, la promesse n'a pas encore été tenue. Sans attendre cet hypothétique grand registre centralisé (qui serait susceptible, comme toute base de données, d'être hacké ou modifié par ses possesseurs), plusieurs écoles d'informatique enregistrent déjà les diplômes de leurs étudiants sur la blockchain, ou plus précisément, leur empreinte numérique unique, le hash. C'est le cas de l'École supérieure d'ingénieurs Léonard-de-Vinci (Esilv), installée sur le parvis de la Défense, et de la Holberton School, une toute jeune institution fondée par deux développeurs français, Sylvain Kalache et Julien Barbier, à San Francisco. La procédure de vérification d'un diplôme est très simple, comme l'explique Cyril Grunspan, le responsable du département d'ingénierie financière de l'Esilv, à l'origine de ce projet mené en collaboration avec Paymium : « L'étudiant peut aller sur le site diploma.report, choisir l'école Esilv, promotion 2015. Il entre son prénom et son nom, et tombe alors sur une page qui indique notamment le hash du diplôme. Il peut envoyer à son futur employeur un lien vers une version publique de cette page, ainsi que la version numérisée de son diplôme. L'employeur pourra vérifier, sur le site, que le hash du diplôme fourni est bien celui enregistré dans la blockchain. » Le document est donc authentique. « L'étudiant peut ainsi prouver sa bonne foi en un clic, et l'employeur n'a plus besoin de nous appeler pour savoir si le diplôme reçu est bidon ou non. Il dispose d'une preuve irréfutable », se félicite Cyril Grunspan, qui compte désormais inscrire chaque promotion diplômée sur la blockchain.

À 9 000 km de là, à San Francisco, le cofondateur de la Holberton School, Julien Barbier, a fait appel à la start-up Bitproof pour certifier les diplômes de sa jeune école. Il voit un grand potentiel à ce type d'application : « Pour les entreprises, cela offre un gain de temps incroyable pour vérifier des diplômes des candidats. Elles n'ont plus besoin d'appeler les universités ou de confier la tâche à une entreprise pour le faire, ce qui peut être coûteux, comme nous l'a confirmé un recruteur. Pour nous aussi, cela nous fait gagner du temps, car nous n'avons pas à répondre aux appels des recruteurs », précise-t-il. « Enfin, nos étudiants sont enchantés de savoir que leurs certificats seront stockés de façon sécurisée dans la base de données du futur, la blockchain. Ils voient que l'industrie du numérique se tourne massivement vers la blockchain et sont fiers de faire partie d'une des premières écoles à l'utiliser[34] », se réjouit-il.

À ces premières expériences isolées menées directement par des écoles s'ajoutent des initiatives plus larges, comme celle du géant japonais Sony. En février 2016, sa filiale dédiée aux services d'éducation, Sony Global Education, a annoncé sa volonté de bâtir une plateforme permettant aux établissements d'enseignement supérieur d'enregistrer sur la blockchain les diplômes et notes aux examens de leurs étudiants. Dans un premier temps, le service accueillera les résultats des 150 000 participants du concours mondial de mathématiques organisé par Sony. L'enjeu, à long terme, est immense : bâtir l'équivalent d'une plateforme de CV, comme LinkedIn ou Viadeo, où les informations seraient 100 % fiables et vérifiées, comme celles d'une carte d'identité. Pour les recruteurs et les candidats, un tel service apporterait une énorme valeur ajoutée. La start-up française Ledgys, spécialisée dans la revente sécurisée de données *via* la blockchain Ethereum, y travaille. Dans un premier temps, elle a lancé Dipl.me : cette application, similaire à celles développées par Paymium et Bitproof pour l'Esilv et Holberton School, se propose de certifier des diplômes des étudiants, après validation de l'information par leur école. Mais le fondateur de Ledgys, Quentin de Beauchesne, voit plus loin : « Nous avons réfléchi à une plateforme qui permettrait d'héberger des données privées et de pouvoir se les vendre. Nous sommes par exemple en train de cocréer une application de vente de compétence : quand un salarié quitte une entreprise, son ex-employeur certifie les compétences acquises. Il n'a ainsi plus besoin de répondre au nouvel employeur pour confirmer que l'ex-employé a bien les qualifications indiquées dans son CV. Le but, c'est de se débarrasser de cette partie administrative et fastidieuse du travail de recrutement[35] », explique-t-il. Les anciens employeurs seront incités à jouer le jeu : « Valoriser leur ex-employé va leur permettre de gagner du temps et de l'argent, par la revente des données qu'ils acceptent d'authentifier. Le futur employeur va payer l'appli et l'appli va reverser une partie à l'ancien employeur. Il y a un vrai marché », déclare Quentin de Beauchesne, enthousiaste.

De multiples autres applications possibles

Les services de notarisation de documents sur la blockchain, à des fins d'authentification, ont d'innombrables autres usages possibles. En France, l'Institut national de la propriété industrielle, qui reçoit les dépôts d'inventions depuis 1951, a commandé, en avril 2016, une étude sur l'impact de la

blockchain dans le domaine de la propriété intellectuelle, dont les résultats devaient être annoncés début 2017. Certains, comme le consultant Éric Lévy-Bencheton, imaginent d'autres applications possibles pour authentifier les documents administratifs souvent falsifiés, comme les quittances EDF ou de loyer. À Paris, les bulletins de paie, pièces essentielles de dossier de location, sont régulièrement modifiés à la hausse par les locataires. Enregistrer leur empreinte unique sur la blockchain permettrait au bailleur d'avoir la certitude de leur authenticité. Les assureurs, comme Axa, travaillent de leur côté à des certifications de couverture sur la blockchain, qui faciliteraient, accéléreraient, voire automatiseraient les contrôles de police. « Aujourd'hui, une assurance auto se représente par un petit papier vert. On pourrait dématérialiser cette preuve assurance, l'enregistrer dans une blockchain et la mettre à disposition des autorités publiques[36] », suggère Laurent Benichou, d'Axa. « Cela pourrait permettre aux autorités de repérer des véhicules non assurés pour les extraire rapidement de la voie publique, et éviterait aux automobilistes de recevoir des contraventions malheureuses s'ils oublient de remplacer le papier vert d'une année sur l'autre » ajoute l'expert.

Enfin, une dernière utilisation, aux conséquences particulièrement vertigineuses, est envisageable : la certification de signatures dans la blockchain. Or que fait-on avec deux signatures ? Un contrat. La blockchain pourrait donc être le lieu idoine où signer des contrats 100 % en ligne, comme le parie Louison Dumont. Après avoir développé Bitproof, il a créé Peter, un « robot avocat », sous la forme d'une application en ligne, dotée d'un système de signature numérique qui permet d'enregistrer un contrat, établi par mail, sur la blockchain. Mieux encore, en utilisant l'intelligence artificielle, Peter[*6] rédige lui-même le contrat demandé de façon automatique, selon les instructions transmises par mail par le client. « Avec Peter, je vends à la fois du conseil légal et un système de signature en ligne super efficace, qui permet de signer directement un e-mail[37] », résume Louison Dumont. Création d'entreprise, levée de fonds… L'application répond à toutes les questions qui concernent le droit des start-up aux États-Unis. « Il suffit d'écrire sa demande par e-mail à peter@peter.ai. Par exemple, Peter, voici l'investisseur auprès de qui on lève 200 000 dollars, est-ce que tu peux nous faire un contrat avec ces termes, doublé d'un contrat de confidentialité ? Peter va alors le générer et l'envoyer », indique Louison Dumont. Quand Peter ne sait pas répondre, des collaborateurs humains prennent le relais. Mais Peter apprend alors de cette défaillance et sait donner la réponse adaptée quand la même requête est présentée la fois suivante. « Techniquement, ça marche. Et comme Peter apprend de ses erreurs, ça fonctionne même de mieux en mieux », assure Louison Dumont, qui envisage d'étendre petit à petit son service à d'autres pays. Seul hic, la loi, aux États-Unis comme ailleurs, ne reconnaît pas encore ce type de signature numérique sur la blockchain. « Mais c'est une preuve scientifique, que l'on peut soumettre à un juge en cas de litige », insiste-t-il. En attendant la première jurisprudence qui accordera une vraie valeur de preuve aux informations stockées sur la blockchain.

---

*1. Et donc de savoir s'il n'a pas été changé.

*2. Forces armées révolutionnaires de Colombie.

*3. National Health Service (NHS).

*4. « Mon nom est Stéphane Loignon et je signe le contrat n° 99b7-bacb-f158-7e45. »

*5. Higher Education Degree Datacheck (HEDD).

*6. https://hirepeter.com/

TROISIÈME PARTIE

LES DÉFIS DE LA BLOCKCHAIN

La blockchain n'en est qu'à ses débuts. Malgré le potentiel que de plus en plus de gens lui reconnaissent, elle fait face à des défis énergétiques, techniques, commerciaux, réglementaires et éthiques qui peuvent paraître insurmontables, dans l'état actuel de la technologie, de la législation et du marché. « La blockchain, pour le moment, est un peu comme Arpanet[*1] à l'égard d'Internet[1] », compare Gilles Babinet, le représentant de la France sur les questions numériques à la Commission européenne[*2]. « La technologie n'est pas encore utilisable à grande échelle, on n'a pas encore trouvé l'équivalent pour la blockchain de TCP/IP[*3] », ajoute-t-il.

Les problèmes sont identifiés. « Les deux principaux sont l'absence de temps réel et la taille du registre, qui exige un niveau de consommation d'énergie très important », estime Gilles Babinet. La fondation Ethereum y travaille activement. « Vitalik Buterin a fixé trois objectifs à Ethereum pour l'année 2017 », confie sa directrice, Ming Chan. « D'abord, la mise à l'échelle, c'est-à-dire la possibilité de faire un bien plus grand nombre de transactions ; ensuite, le passage d'un système de validation *proof of work* à un mode *proof of stake*, pour éviter de gâcher autant d'électricité pour le minage ; enfin, régler d'autres problématiques comme la demande émise par beaucoup d'entreprises d'une plus grande confidentialité[2]. » Les nombreux développeurs d'Ethereum y travaillent. Ils ne sont pas les seuls. Partout dans le monde, des chercheurs et des entrepreneurs de talent dans des universités, des start-up et des grands groupes s'attellent également à trouver des réponses ingénieuses et pratiques à ces défis. Le jeu en vaut la chandelle : un nouveau monde est à portée de code.

CHAPITRE 8

Développer des systèmes moins énergivores

Le principal obstacle à la démocratisation de la blockchain est la consommation d'énergie assez colossale que le minage des transactions exige pour le moment. Les deux principales blockchains publiques, Bitcoin et Ethereum, fonctionnent à ce jour avec des systèmes de validation en preuve de travail (*proof of work*) : cette méthode mobilise les capacités de calcul de tous les nœuds du réseau, qui mènent une course pour résoudre en premier le problème mathématique posé, valider la transaction et être récompensé par quelques Bitcoins ou Ethers. Une chose est sûre, c'est beaucoup d'énergie dépensée pour valider un bloc. Combien exactement ? Les estimations, fondées sur la consommation des sociétés spécialisées dans le minage, divergent assez fortement. En mars 2016, un chercheur néerlandais, Sebastiaan Deetman, évaluait, dans un article publié sur le site Motherboard, que la blockchain Bitcoin consommait environ 300 mégawatts (MW)[1]. Une dépêche de l'AFP d'août 2016 proposait un chiffre deux fois supérieur : « La blockchain du Bitcoin qui pèse aujourd'hui 78 gigaoctets consomme aux alentours de 600 MW d'énergie pour fonctionner, soit un cinquième de la capacité de la centrale nucléaire d'EDF en projet à Hinkley Point (3 200 MW)[2]. » Si aucune solution n'est proposée, la démocratisation progressive du Bitcoin et des autres cryptomonnaies ne fera qu'empirer la situation. D'après les calculs de Sebastiaan Deetman, au rythme actuel de croissance du réseau Bitcoin, il devrait absorber, en 2020, l'équivalent de la consommation énergétique du Danemark.

Cette consommation abondante se traduit par de lourds investissements faits par les sociétés de minage dans des hangars remplis d'ordinateurs et de matériel informatique. Ils sont installés là où l'électricité et l'équipement sont les moins chers : en Chine en particulier, mais aussi en Europe, dans les Alpes suisses (pour les serveurs de Bitcoin Suisse), dans les Pyrénées (pour ceux de BTC facil) ou encore en Islande. Dans un article de *Business Insider*[3], Marco Streng, le PDG de Genesis, une firme de minage installée sur l'île, a déclaré que les compagnies énergétiques lui offraient des tours en

hélicoptère, car sa société était devenue l'un des principaux consommateurs du pays. Cette pratique est problématique sur le plan environnemental : plus de 70 % du minage a lieu en Chine[*1], un pays où la production d'électricité se fait surtout dans des centrales au charbon, très polluantes et émettrices de CO^{42}. Elle constitue aussi une barrière à l'entrée dans le secteur, supposément ouvert, du « mining », qui n'est plus à la portée du premier venu. « Être mineur aujourd'hui, c'est investir des millions de dollars dans des fermes de serveurs paramétrés et optimisés dans ce but », commente Alain Brégy, d'Aedeus. Le problème, c'est que l'industrie numérique en général consomme déjà beaucoup : « Chez Facebook, les data centers et leur besoin en énergie sont de très loin le premier poste d'exploitation », affirme Gilles Babinet. Dans ce contexte, ajoute l'expert, « vous ne pouvez pas débarquer avec une nouvelle technologie qui a pour caractéristique d'être très énergivore. Si un objet connecté est optimisé pour consommer peu, mais que le système derrière consomme beaucoup, ça ne fonctionne pas ».

L'équation n'est pas facile à résoudre car c'est le choix de la distribution de l'information, plutôt que de la centralisation qui est l'origine de cette surconsommation : « Un système qui repose sur un registre distribué consomme beaucoup plus qu'un système client-serveur, car vous démultipliez les besoins de traitement de données », insiste Gilles Babinet. Des pistes de solutions existent. Celle généralement proposée est de changer le système de validation et de renoncer au *proof of work*, trop dispendieux. Suivant les cas d'usage, toutes les blockchains n'ont pas besoin d'une validation en preuve de travail, souligne François Dorléans, de Stratumn : « Pour faire travailler trois entreprises ensemble, pas besoin de *proof of work* », juge-t-il. Une blockchain privée, où l'acceptation des transactions est déléguée à un ou plusieurs validateurs désignés, suffit. C'est par exemple le cas sur la blockchain de Revelator, la start-up musicale de Bruno Guez. Mais il s'agit alors de systèmes dans lesquels il faut à nouveau faire confiance à un intermédiaire, ce que promettait d'abolir la blockchain d'origine, Bitcoin. Pour les blockchains publiques, l'alternative à la preuve de travail est la preuve d'enjeu, ou *proof of stake*, qui ne demande pas d'effort de calcul. En 2015, la blockchain SolarCoin, conçue pour promouvoir l'énergie propre, a ainsi décidé d'abandonner le mode *proof of work* pour le *proof of stake* qui, selon la fondation SolarCoin, présente « l'avantage d'avoir une empreinte-carbone nettement réduite par rapport au POW, avec une réduction potentielle de 99,9 % des ressources informatiques nécessaires pour faire circuler la monnaie[5] ». Mais le *proof of stake* a, lui, d'autres inconvénients de taille : c'est celui qui détient le plus de cryptomonnaie, donc le plus puissant financièrement, qui exerce le plus de contrôle sur le réseau (ce qui pose un problème de confiance et de sécurité). Pour le moment, aucun système n'allie à la fois le même degré de décentralisation que le Bitcoin et une consommation d'énergie plus raisonnable. « Beaucoup de chercheurs travaillent là-dessus », précise Gilles Babinet. Laissons-leur le temps d'avancer. « La communauté est au courant du problème. Je ne me fais pas de souci sur le fait que des solutions vont être apportées[6] », a déclaré Antoine Yeretzian, le cofondateur de Blockchain France, lors du Forum parlementaire de la blockchain.

*1. Auprès de quatre principales sociétés : F2Pool, Antpool, BTCC Pool et BW.com.

CHAPITRE 9

Rapidité, confidentialité, sécurité : trois défis techniques

Plusieurs autres défis techniques devront être surmontés pour permettre le succès de la technologie blockchain auprès du grand public.

Accélérer le traitement des transactions

Le premier est celui de la rapidité. Ce problème se pose principalement sur la blockchain la plus utilisée, le Bitcoin, où la taille des blocs est limitée à 1 MB et où ces derniers sont validés toutes les 10 minutes. Résultat : seules 7 transactions au maximum peuvent avoir lieu à chaque seconde, contre en moyenne 200 dans le système Paypal [1] et 2 000 chez Visa. La communauté Bitcoin a débattu longuement en 2016 de l'opportunité d'accroître la taille des blocs, pour accélérer le processus, mais n'a finalement pas mis en œuvre ce changement pour l'instant. « Le Bitcoin est un truc d'amateur un peu génial, il est aujourd'hui victime de son succès. Pour l'instant ça va, mais on ne peut pas se mettre à faire tous les achats de la planète sur le Bitcoin », juge Cyril Grunspan, de l'Esilv. Des solutions existent. L'une d'entre elles consiste à faire des « sidechains » : des blockchains séparées, qui permettent de décongestionner la blockchain principale et gardent un lien avec elle. L'autre solution, retenue par les blockchains rivales du Bitcoin, est d'adopter un mode de validation plus simple, comme l'a choisi Revelator : « Sur notre propre blockchain, on peut gérer 3 000 transactions par seconde. Pour les micropaiements il est nécessaire d'avoir une infrastructure qui va pouvoir vraiment soutenir la croissance », insiste le fondateur Bruno Guez.

Le dilemme de la transparence et de la confidentialité

Le deuxième grand défi est celui de la confidentialité. Sur les blockchains publiques, comme Bitcoin ou Ethereum, l'ensemble des transactions est visible. La seule protection pour préserver la discrétion d'une opération est apportée par les pseudonymes, sous forme de clés publiques, qui masquent les identités réelles de participants. Pour beaucoup d'entreprises, ce n'est pas suffisant. Immergées dans des univers compétitifs, elles ne peuvent pas se permettre de donner trop d'informations à leurs rivales. Si leur pseudonyme était démasqué, des concurrents pourraient retracer l'intégralité de leur historique de transactions. Une éventualité tout bonnement inenvisageable pour beaucoup de chefs d'entreprise. Il y a des solutions : *a minima*, changer régulièrement de clés publiques (pseudonymes), comme Paymium le fait pour ses clients. Ensuite, certaines opérations peuvent avoir lieu sur des « sidechains » privées. Le détail des transactions ayant eu lieu dans cette bulle privée n'apparaît alors pas dans la blockchain publique. En dernier recours, la plus grande garantie de protection de la confidentialité est la blockchain privée. « Des entreprises comme MTV, la BBC ou RTL n'ont aucun intérêt à poster toutes leurs transactions sur la blockchain Bitcoin, c'est pourquoi nous construisons des blockchains privées », justifie Bruno Guez. Le même raisonnement est valable dans de nombreux secteurs, dont la finance, où seuls les projets de registres distribués privés intéressent les banques.

Certains universitaires élaborent des solutions expérimentales pour conserver la publicité des transactions – condition d'un système décentralisé où chacun peut valider une opération – et une meilleure protection des données privées. Ancien chercheur au MIT, Guy Zyskind a ainsi cofondé Enigma, une start-up qui veut permettre aux blockchains publiques existantes d'offrir la confidentialité dont elles manquent. « Enigma permet de traiter les données sans les voir[2] », résume Guy Zyskind. « Vous pouvez toujours prouver quelque chose, le vérifier, profiter de la transparence, mais sans révéler d'information sensible. Cela semble contre-intuitif. Comment pourrais-je dire qu'une transaction est correcte si je ne vois pas les fonds ? La solution est assez complexe, mais elle existe : cela s'appelle le calcul multiparties[*1]. » La méthode implique notamment le cryptage des données, dont l'intégralité brute n'est jamais dévoilée à aucune des parties. La solution est prometteuse, et pourrait trouver des débouchés dans les domaines où la confidentialité, primordiale, bloque pour l'instant l'utilisation des données : « par exemple la recherche médicale, car pour l'instant, il est très difficile de partager des informations entre hôpitaux ou entre laboratoires pharmaceutiques ».

Sécuriser les blockchains et les plateformes d'échange

Le dernier grand défi technique posé aux développeurs d'applications blockchain est celui de la sécurité. C'est un point décisif, car en l'absence de banque centrale, toute la valeur des cryptomonnaies dépend de la confiance qui leur est accordée. Si des doutes persistent sur la fiabilité d'un registre distribué de transactions, ses jetons ne valent plus rien. Or le succès des blockchains suscite la

convoitise. Plus il y aura d'argent en jeu, plus des pirates seront tentés de trouver des failles pour détourner des cryptomonnaies. Il existe deux grandes catégories de failles : la première concerne non pas la blockchain directement, mais l'accès à celle-ci. Quand vous achetez des Bitcoins, des Ethers ou toute autre monnaie numérique pair à pair, vous passez en général par un intermédiaire : une plateforme d'échange (ou une banque Bitcoin qui passe ensuite par une plateforme d'échange). Celle-ci est susceptible d'enregistrer vos informations personnelles dans une base de données (e-mails, identifiants, mots de passe, clé publique, voire clé privée), qui peut être hackée, ou modifiée par ceux qui détiennent la base à leur profit. Sans que l'on sache toujours exactement comment, pas moins de 850 000 Bitcoins [*2] ont disparu, en février 2014, de la plateforme japonaise MtGox, qui était alors l'un des principaux lieux d'échange de Bitcoins au monde. Plus récemment, en août 2016, 120 000 Bitcoins [*3] ont été subtilisés à Bitfinex, l'une des principales bourses de Bitcoin. Selon une estimation de l'agence Reuters, un tiers des plateformes d'échange ont été hackées depuis 2009 [3]. « Les banques en ligne se font hacker presque tous les jours [4] », relativise Pierre Noizat, le fondateur de Paymium. De même qu'un voleur peut braquer une banque ou cambrioler un appartement, des pirates peuvent aussi s'attaquer, tout simplement, à votre propre ordinateur, par un logiciel espion, qui récupérera vos clés d'accès. Il existe une façon simple de s'en prémunir, en conservant ses identifiants, mots de passe ou clés de préférence sur papier, et éventuellement en les cachant.

Le second grand type de risque est celui d'un piratage de la blockchain elle-même. Celle du Bitcoin est très robuste et n'a jamais été piratée en sept années d'existence [*4]. « Sur le Bitcoin, tous les casses ont eu lieu au péage, il n'y en a jamais eu sur l'autoroute [5] », précisait Philippe Dewost, de la Caisse des dépôts et consignations, lors du Forum parlementaire de la blockchain. Un casse « sur l'autoroute » ne pourrait avoir lieu que si une personne ou un groupe de personnes alliées contrôlaient strictement plus de 50 % de la puissance du réseau. Elles pourraient alors être choisies suffisamment régulièrement pour valider de façon durable une succession de transactions incorrectes. Ce n'est jamais arrivé, mais la concentration des fermes de mining pourrait poser problème, si par exemple les quatre sociétés chinoises qui dominent le secteur décidaient de s'allier pour truquer le système. Elles n'y ont toutefois pas intérêt, car une telle attaque détruirait la confiance des usagers dans le Bitcoin et ferait plonger pour de bon la valeur de la monnaie. La blockchain d'Ethereum, au code plus complexe, donc plus faillible, n'affiche pas la même solidité.

À l'inverse du Bitcoin, son code est *turing complete*, comme disent les experts : il permet de faire des boucles, c'est-à-dire des programmes qui s'exécutent à l'infini. Cela ouvre d'immenses possibilités commerciales pour automatiser des opérations, mais cela crée aussi des opportunités pour des hackers malveillants, qui peuvent inscrire un *smart contract* pour détourner de l'argent, jusqu'à la fin des temps. « Le langage *turing complete* ouvre la possibilité aux bugs et aux malwares (programmes malveillants). Si je veux détruire Ethereum, je peux envoyer un contrat qui tourne jusqu'à capter toutes les ressources. Ça tuerait cette cryptomonnaie [6] », commente Nicolas Houy, économiste au CNRS. La mésaventure du fonds participatif TheDAO, en juin 2016, a servi d'avertissement. « Un bug dans un contrat a permis cette attaque. Cela a rappelé que ce qui peut être programmé peut aussi être hacké. Avec 150 millions de

dollars en jeu, il était évident que cela allait attirer des pirates », commente Simon Polrot, le fondateur du site Ethereum France.

C'est en fait une question de fond qui divise partisans du Bitcoin et d'Ethereum : est-il possible de créer une blockchain plus performante que celle du Bitcoin – plus facilement programmable et plus rapide – et aussi sécurisée ? « Le Bitcoin, ça a été bien étudié, testé pendant sept ans. De toutes petites modifications [*5] peuvent avoir d'énormes conséquences », estime Nicolas Houy. Pour Pierre Noizat, grand défenseur du Bitcoin, « la sécurité est antagoniste de la performance et de la praticité. Il y a une contradiction entre la volonté de faire une machine virtuelle haute performance pour plein d'applications différentes et celle de faire du paiement avec les Ethers ». C'est le défi que devront relever les développeurs d'Ethereum. Une chose est sûre : la débâcle de TheDAO a montré à quel point il était indispensable que le code soit audité avec la plus grande rigueur, car la moindre faille peut coûter très cher.

---

*1. « Multi-party computation. »

*2. L'équivalent de 660 millions de dollars au cours du 10 décembre 2016.

*3. L'équivalent de 93 millions de dollars au cours du 10 décembre 2016.

*4. Le 8 août 2010, un bug majeur avait toutefois été découvert et vite résolu par la communauté des développeurs.

*5. Comme la possibilité de programmer des boucles.

CHAPITRE 10

Marketing : trouver des modèles économiques viables sans se renier

La puissance du concept de blockchain repose sur la désintermédiation : elle est l'outil d'une émancipation du consommateur vis-à-vis des banques et des géants du Web. Cela posé, faire des affaires avec la blockchain est difficile. Start-up et grands groupes veulent gagner de l'argent. Il existe donc un vrai défi marketing et commercial, consistant à trouver des modèles économiques rentables, tout en respectant ce qui fait la valeur de la blockchain : la décentralisation, la transparence et l'immutabilité de ce qui y est inscrit.

Les grands groupes veulent conserver leur avantage

Pour les grands groupes, dont les traditionnels modèles économiques centralisés sont attaqués par cette technologie, l'exercice est presque contre-nature. La transparence, en particulier, pose problème, si bien que la plupart des projets menés par les banques (par exemple le consortium R3) ou par les grands noms de la technologie (IBM avec Hyperledger) sont des blockchains privées, où la transparence est limitée. L'immutabilité aussi gêne certains. En septembre, le cabinet Accenture a ainsi conçu une blockchain « éditable », c'est-à-dire pouvant être réécrite par un administrateur central (une hérésie aux yeux de beaucoup dans le secteur de la blockchain). Enfin, la décentralisation n'est pas à leur avantage : les banques n'ont pas envie de disparaître, les compagnies d'assurances n'ont pas l'intention d'être remplacées pas des mutuelles pair à pair, les géants du cloud veulent conserver la position de force que leur donne la maîtrise des données des internautes. L'intérêt porté par les compagnies d'assurances à la mutuelle blockchain pair à pair Wekeep.io est emblématique : « Ça les intéresse beaucoup de comprendre ce qu'on fait, mais ils nous disent qu'ils n'ont pas de budget à mettre là-dedans. Ils veulent

faire de l'innovation incrémentale[*1], améliorer leur business, pas faire de l'innovation de rupture[1] », témoigne le créateur du projet, Adrian Sauzade. Malgré tout, certaines sociétés arrivent à se réinventer pour imaginer des services blockchains qui apportent une vraie valeur au consommateur. Les projets menés par IBM, pour relier blockchain et objets connectés, ou ceux d'assurance automatique d'Axa, sont prometteurs. La blockchain peut faire émerger de nouvelles opportunités, comme le suggère l'expert numérique de la mutuelle française Maif, Erik Arnaud : « Si vous perdez la clé privée de votre portefeuille de cryptomonnaie, vous n'avez plus d'accès à rien. Il y a un besoin de tiers de confiance pour garantir et sécuriser l'accès à la blockchain de l'économie réelle », estimait-il lors des débats du Forum parlementaire de la blockchain.

Vers de nouveaux intermédiaires ?

Le plus probable est néanmoins que les vraies innovations de ruptures soient plutôt amenées par des start-up que par des acteurs installés, qui seront tentés de conserver le plus longtemps possible leur position de force. C'est ce qui s'est passé, jusqu'à maintenant, dans l'économie d'Internet, où la plupart des grandes vagues d'innovation ont été portées par des nouveaux entrants (à l'exception notable d'Apple avec l'iPhone). En suivant cette logique, le destin de la blockchain est dans les mains des entrepreneurs, et non des laboratoires d'innovation de grands groupes. Mais encore faut-il qu'ils conservent leur indépendance. « Désormais, les développeurs de Bitcoin se font embaucher entre 5 000 et 10 000 euros par mois pour travailler dans les banques et des compagnies d'assurances, au lieu de créer des start-up », regrette Laurent Leloup, le fondateur du site Finyear. Ce n'est pas le cas de tous, heureusement.

Mais les start-up aussi font face à un écueil : elles peuvent être tentées de devenir de nouveaux intermédiaires, remplaçant les anciens. Ainsi Arcade City, le rival blockchain d'Uber, prévoit-il pour le moment de prélever une commission sur les trajets des chauffeurs : celle-ci est inférieure à celle prélevée par Uber (10 % contre 25 %), mais le système n'est pas véritablement pair à pair. Certaines officient déjà comme intermédiaires entre le consommateur et la blockchain, comme Paymium ou la Maison du Bitcoin, qui facilitent l'acquisition de devises numériques. Cette intermédiation n'est pas forcément problématique, tant que le consommateur s'y retrouve. Notons qu'elle n'est pas la seule manière possible de gagner de l'argent sur la blockchain. Un nouveau modèle émerge : certains développeurs créent des plateformes ouvertes, gratuites, authentiquement pair à pair, et se rémunèrent en proposant des services sur celles-ci. C'est le cas de la société OB1, du fondateur d'OpenBazaar, ou des créateurs du marché prédictif Augur, dont la plateforme est libre d'accès et qui espèrent se rémunérer comme « rapporteurs », en validant les résultats des paris. Finalement, véritables blockchains et business ne sont donc pas antinomiques : des modèles *open source* peuvent fonctionner et les intermédiaires sont tolérés tant qu'ils apportent vraiment de la valeur ajoutée.

Est-il alors naïf de croire à la grande désintermédiation promise par la blockchain ? La plus probable est que la blockchain bouscule les positions de force établies dans l'économie numérique et la

finance, qu'elle élimine des points de blocage inutiles dans l'exécution d'un service, mais qu'elle laisse toutefois de la place à des intermédiaires : soit d'anciennes compagnies traditionnelles qui auront su inventer des services pertinents, soit de nouvelles start-up qui auront créé les applications distribuées que nous utiliserons. « Les gens aiment les intermédiaires malgré tout, ils aiment bien déléguer. La blockchain résout des fonctionnalités de base, mais il y a besoin d'énormément de travail avant qu'elle n'arrive à tout remplacer », estime Primavera De Filippi. La désintermédiation absolue, au profit d'une économie entièrement pair à pair, est une chimère. Dans l'énergie, un intermédiaire assumant la responsabilité de distribuer le courant restera nécessaire, même dans un *smart grid*. « Dans ce secteur, les conséquences sont graves quand quelque chose se passe mal. Cela ne peut pas être totalement décentralisé, on a toujours besoin d'une forte autorité centrale, qui garantit la sécurité », estime John Lilic, l'expert énergie de la firme américaine Consensys. Pour le fondateur de cette start-up, Joseph Lubin, « la blockchain va surtout réduire les barrières à l'entrée pour devenir l'un de ces intermédiaires. Elle va diminuer la valeur captée par ces derniers et accroître la vélocité des industries concernées, en poussant les acteurs à apporter plus de valeur qu'ils n'en prélèvent. Cela crée une compétition plus large et des systèmes plus fluides. Il sera incroyablement difficile de maintenir un monopole. En éliminant les frictions, la blockchain va promouvoir des marchés libres et décentralisés ».

---

*1. Progressive.

CHAPITRE 11

Transformer l’emploi sans le détruire

En sécurisant les communications et transactions entre objets connectés, la blockchain devrait renforcer le vaste mouvement, déjà à l’œuvre, d’automatisation d’un nombre toujours plus grand de métiers. Elle devrait aussi en créer de nouveaux. Mais il est à craindre que ces derniers ne compensent pas les pertes d’emploi dues à la robotisation.

Extension du domaine de l’automatisation

Dans la finance par exemple, les milliards d’euros d’économies qu’espèrent les banques proviennent de la disparition de processus entiers (de vérification, de compensation, d’audit, etc.), qui se traduiront par des suppressions de postes. Les notaires ont aussi du souci à se faire, voire les avocats. « Le métier d’avocat ne va pas disparaître[1] », tempère Simon Polrot. « Dans un monde de *smart contracts*, la connaissance juridique de l’avocat restera nécessaire, pour les concevoir et pour conseiller lors d’un litige. Mais il faudra comprendre la logique informatique et la programmation pour déchiffrer ou composer ce genre de contrats », admet-il. À ce jour, il n’existe aucune étude d’impact de la blockchain sur l’emploi. Mais il en existe sur les conséquences de l’automatisation permise par la connexion des objets et l’intelligence artificielle. En novembre 2015, le cabinet de conseil McKinsey avait publié un article alarmiste, qui estimait que « 45 % des activités que les individus sont payés à faire peuvent être automatisées en adaptant des technologies existantes[2] ». La blockchain renforce la crédibilité de ce pronostic et certains, parmi ceux qui la promeuvent, en sont bien conscients.

Du haut de ses 19 ans, Louison Dumont, qui développe son robot avocat Peter doté d’intelligence artificielle, a de grandes ambitions : « Ma vision de long terme, c’est de supprimer le travail. Je veux que les gens n’aient plus besoin de travailler et que tout le monde soit un artiste[3]. » L’idée n’est pas si folle.

Louison Dumont est soutenu dans ses projets par l'un des plus grands investisseurs de la Silicon Valley, Tim Draper (qui a précédemment misé sur Hotmail, Skype ou Tesla). Sa vision d'un monde où l'homme serait libéré du fardeau du travail fait écho à celle exprimée par l'économiste britannique John Maynard Keynes, dans sa *Lettre à mes petits enfants*, publiée en 1931. À ses yeux, il ne fallait pas s'inquiéter de cette automatisation croissante du travail, mais l'accueillir comme une opportunité d'émancipation : « Dans très peu d'années – j'entends au cours de notre propre existence – il nous sera sans doute possible d'accomplir tous les actes que demandent l'agriculture, l'extraction des mines et la fabrication des objets en ne fournissant que le quart des efforts auxquels nous sommes habitués. L'extrême rapidité de ces bouleversements nous blesse. Nous sommes atteints d'un nouveau mal : le chômage technologique […]. Mais il n'y a là qu'un état temporaire de réadaptation. Tout cela signifie, en fin de compte, que l'humanité est en train de résoudre le problème économique […]. Pour la première fois depuis ses origines, l'homme se trouvera face à face avec son véritable, son éternel problème – quel usage faire de sa liberté, comment occuper les loisirs que la science et les intérêts composés lui auront assurés, comment vivre sagement et agréablement, vivre bien[4] ? »

Une révolution du management

Parallèlement à ce phénomène d'automatisation, la blockchain entraîne un second changement dans le monde du travail : elle favorise l'association de travailleurs indépendants, qui pourront se regrouper dans des organisations décentralisées (les DAO), sans chef, aux règles clairement fixées dans le code de *smart contracts*. « Les individus peuvent faire ces systèmes de coopératives, où ils obtiennent, par leur contribution à un projet, non pas un salaire, mais un titre, une action, quelque chose dont la valeur dépend de celle du projet[5] », précise la chercheuse Primavera De Filippi. « La valeur est ainsi distribuée de manière bien plus équitable qu'aujourd'hui dans ce qu'on appelle l'économie collaborative [Uber, Airbnb], où un acteur capte la valeur richesse par la collaboration des autres », ajoute-t-elle. Dans ces DAO, plus besoin d'empiler les couches de management : les chefs ont disparu, la coordination est assurée par le code.

C'est la vision qu'en donnait Vitalik Buterin, dès la fin de 2013. Pour lui, l'automatisation ne menace pas tant les exécutants des tâches que les donneurs d'ordre, devenus superflus dans des DAO bien conçues : « Si nous avons encore besoin d'humains pour réaliser certaines tâches, peut-on faire disparaître le management de l'équation ? La plupart des entreprises formulent ce qu'est leur mission : souvent, il s'agit de faire gagner de l'argent aux actionnaires ; parfois s'y ajoute une sorte d'impératif moral lié au produit qu'elles créent, ainsi qu'éventuellement d'autres objectifs comme aider les communautés, au moins en théorie. Actuellement, cette mission d'entreprise n'existe que par l'interprétation qu'en font le comité exécutif et *in fine* les actionnaires. Mais que se passerait-il si, grâce à la puissance des technologies modernes de l'information, nous pouvions traduire cette mission dans du code ; c'est-à-dire créer un contrat inviolable qui génère du chiffre d'affaires, paye les gens pour

accomplir certaines fonctions, et trouve de lui-même le matériel pour fonctionner, tout cela sans aucun besoin de management vertical humain[6] ? »

Cette vision de la DAO, comme une coopérative où le management est remplacé par du code, trouve sa première traduction concrète dans les projets menés par la start-up française Open Org et l'israélienne Backfeed. Le fondateur d'OpenOrg.co, Louis Margot-Duclot, conseille des entreprises qui veulent rendre leur processus de gouvernance plus ouvert et transparent. Il leur propose de se réorganiser comme des plateformes de gouvernance de projet, qu'il appelle des « sociétés ouvertes » : chaque projet est découpé en une liste de tâches, auxquelles un certain temps nécessaire à l'exécution et une rémunération sont alloués. Chaque travailleur peut alors choisir et effectuer la tâche pour laquelle il est le plus compétent. « Traditionnellement, c'est un manager qui assigne les tâches. Dans notre modèle, c'est un employé qui se l'assigne. La vérification, habituellement, est faite par le manager. Dans une société ouverte, elle peut être faite soit par le groupe de gens qui a créé la liste de tâches, soit par des gens que l'on aurait désignés pour vérifier l'accomplissement des tâches des autres », explique-t-il. Quand la mission est effectuée, la rémunération correspondante est versée automatiquement en cryptomonnaie. Chaque travailleur devient une sorte de contractant de son employeur… voire d'un autre. « Dans notre vision, la liste de tâches est la plus ouverte possible : elle est publique, sur Internet, et n'importe qui va pouvoir s'en saisir. Chacun est un jour collaborateur de l'entreprise et le lendemain non », ajoute Louis Margot-Duclot. En Israël, Backfeed propose un modèle légèrement différent d'organisation décentralisée, où chaque participant est rémunéré proportionnellement à sa contribution au projet. Son objectif est de proposer un modèle de structure et de règles transcrites dans le code qui permettent de promouvoir la coopération à large échelle, sur tout type de projet. Une première application devrait voir le jour au premier semestre 2017.

CHAPITRE 12

Réglementer sans freiner l'innovation

La blockchain est une technologie complexe, face à laquelle les législateurs sont bien embarrassés. D'un côté, elle est l'instrument de transferts financiers de plus en plus importants, parfois transfrontaliers, et il n'y a pas de raison qu'ils échappent ni à l'encadrement de la loi, ni à la fiscalité. De l'autre, elle est une source d'innovation et de création de valeur qu'aucun pays ne veut étouffer par une règle inadaptée, qui pousserait les start-up à se relocaliser ailleurs. Mais l'absence de règle peut aussi être un frein. Alors, que faire ? Pour l'instant, la réponse donnée par la plupart des législateurs est : pas grand-chose.

Attentisme et prudence

En France, les hommes politiques les plus en pointe sur le sujet, de gauche comme de droite, semblent terrorisés à l'idée de faire une bêtise. « Sur ce sujet-là, moins on en fera, mieux ça sera. Je n'ai pas hâte qu'il y ait une loi Blockchain[1] », lançait Lionel Tardy, député LR de Haute-Savoie, lors du Forum parlementaire de la blockchain, début octobre 2016. « Il ne faut pas légiférer à ce stade, il est beaucoup trop tôt pour mettre un frein à ce genre de technologie[2] », abondait Axelle Lemaire, alors secrétaire d'État au Numérique et à l'Innovation, en conclusion de l'événement. Pour la députée PS des Côtes-d'Armor Corinne Erhel, « il faut d'abord bien comprendre comment cela fonctionne, quels sont les enjeux et les impacts, avant de réguler. Il faut laisser cette technologie se développer, même s'il est vrai qu'elle pose des questions sur la responsabilité et la sécurisation des transactions notamment[3] ».

L'industrie elle-même est divisée sur la nécessité ou non de réglementer plus précisément ces nouvelles technologies. « Il faut définir un cadre réglementaire adapté à cette technologie[4] », considère Nicolas Rivard, responsable de l'innovation chez Euronext Paris. « Pas tout de suite, la blockchain est au début du chemin[5] », répond Luca Comparini, l'expert d'IBM.

En attendant, en l'absence de règles *ad hoc*, le droit existant s'applique. Mais il n'est pas toujours clair de savoir comment. « Aujourd'hui, l'absence d'encadrement freine les acteurs, on ne sait pas si ce qu'on fait est légal ou pas, car il n'y a pas de position claire sur ce qu'est une cryptomonnaie ou sur ce qu'est une preuve cryptographique, par exemple[6] », insiste Simon Polrot, fondateur du site Ethereum France et avocat au cabinet Fieldfisher. Son affirmation est confirmée par une étude récente du cabinet Deloitte et de l'association EFMA : pour 49 % des 3 000 acteurs du monde financier interrogés, la principale préoccupation concernant la blockchain est « la réglementation et les incertitudes légales », loin devant la sécurité (15 %)[7]. La réglementation n'est pas forcément un handicap pour l'innovation, au contraire, comme le prouve l'expérience française. Les deux initiatives légales menées par les autorités hexagonales en 2016 dans le domaine de la blockchain – l'ordonnance sur les minibons du 28 avril et celle sur l'autoconsommation d'énergie – ont ouvert deux nouveaux marchés aux acteurs du secteur, et se sont traduites quelques mois plus tard par des services concrets, lancés respectivement par BNP Paribas (pour les minibons) et par Bouygues Immobilier et Stratumn (pour les microréseaux énergétiques).

Quel statut légal accorder ?

Concrètement, plusieurs questions juridiques se posent. D'abord, celle du statut des cryptomonnaies : doivent-elles être considérées comme des monnaies, auquel cas elles sont exonérées de TVA (taxe sur la valeur ajoutée), ou des biens (sur lesquels la TVA est exigée) ? Un arrêt de la Cour de justice de l'Union européenne, en date du 22 octobre 2015, a décidé de considérer le Bitcoin comme un « moyen de paiement » et d'exonérer ainsi ses échanges de TVA, invalidant ainsi une demande faite par le fisc suédois. Mais son statut (monnaie, actif physique, actif financier…), en France en particulier, ne reste pas clair, si bien que le fisc, mais aussi les douanes et les autorités financières (Autorité des marchés financiers, Autorité de contrôle prudentiel et de résolution) ne savent pas très bien quelle réglementation lui appliquer (ni s'il entre dans leur champ de compétence)[8]. Suivant les pays, les intermédiaires de cryptomonnaies ne sont pas soumis aux mêmes obligations : dans l'État de New York, ils doivent ainsi obtenir une licence spécifique depuis l'été 2015. D'autres États, comme la Suisse, sont moins regardants, et permettent aux start-up financières blockchain d'exercer sans licence bancaire (ni d'aucune sorte).

La deuxième question à trancher est celle de la valeur juridique accordée aux preuves enregistrées sur la blockchain. « S'il fallait faire une réglementation, ce serait pour encourager cette notion de preuve[9] », a déclaré l'avocat Hubert de Vauplane, associé au cabinet Kramer-Levin, lors du Forum parlementaire de la blockchain. « Le politique devra se poser la question de la valeur juridique donnée par certains actes sur la blockchain[10] », admet le député Lionel Tardy. Sans cet adoubement juridique, les si prometteurs services de notarisation n'auront pas de valeur opposable, même quand ils offrent une véritable garantie d'immutabilité. « Pour l'instant, il n'y a pas de marché pour les services comme Bitproof, à cause de ce vide juridique. C'est un des gros problèmes du Bitcoin en ce moment[11] »,

considère son fondateur, Louison Dumont. « Attention toutefois, prévient Claire Balva, la cofondatrice de Blockchain France, toutes les blockchains ne sont pas les mêmes et ne sont pas aussi sécurisées que le Bitcoin[12]. » Le déclic pourrait venir d'une décision d'un tribunal américain, qui ferait jurisprudence aux États-Unis, ce qui ferait décoller ces services outre-Atlantique et pousserait les législateurs européens à embrayer. « Dès qu'un juge américain dira oui, c'est vrai, cette preuve est valable, il y aura une légalisation du stockage d'informations dans la blockchain[13] », espère Manuel Valente, directeur de La Maison du Bitcoin. En France, la députée LR d'Eure-et-Loir, Laure de La Raudière, a fait une première tentative dans ce sens en mai 2016. « J'avais souhaité qu'on introduise dans le code civil la certification d'actes dans des registres distribués[14] », se rappelle-t-elle. Son amendement, prévu dans la loi Sapin 2, donnait une définition juridique des transactions certifiées par la blockchain et leur aurait conféré une valeur équivalente aux inscriptions dans un registre physique. Une transaction enregistrée sur la blockchain aurait eu la même valeur de preuve légale que si elle avait été enregistrée par un office notarial. Mais la disposition s'est heurtée à la résistance du lobby des notaires, et a reçu un avis défavorable. « Ils sont effrayés par la blockchain, car elle remet en cause une partie de leur métier. Ils avaient néanmoins de bons arguments, concède-t-elle, et soulignaient que dans le cadre du droit français, l'inscription dans un registre notarié était toujours accompagnée d'une explication de la position des deux parties et d'une obligation de conseil, ce qui n'est pas le cas sur la blockchain. » Ce n'est sans doute que partie remise. « Il faut avoir un vrai débat avec les notaires sur la mise en place de la blockchain pour des actes aujourd'hui notariés. Le pire serait de se mettre la tête dans le sac et de refuser de voir qu'il existe des technologies nouvelles, c'est dans ces moments-là que l'on prend du retard par rapport à d'autre pays », conclut-elle.

Qui est responsable ?

La troisième grande question légale, fondamentale, est celle de la responsabilité : qui l'endosse, quand un litige survient dans l'utilisation d'une application blockchain publique ? Est-ce celui qui a créé la blockchain ? L'ensemble de la communauté des membres ? Celui qui a créé l'application ? Ceux qui l'utilisent ? Personne ? La logique de la blockchain est de faire reposer la confiance des utilisateurs non pas sur un organisateur central, mais sur du code transparent. « *Code is law* », le code fait loi, comme aiment dire les experts du secteur. Mais que se passe-t-il quand ce code est mal écrit, qu'il y a une faille et qu'un hacker profite de cette faiblesse ? La question s'est posée avec acuité lors du hack de TheDAO. Pour éviter de perdre ses fonds, la communauté des utilisateurs Ethereum avait décidé de revenir en arrière, en opérant un « fork », une réécriture de la blockchain. Pourtant, le hacker n'avait fait qu'exploiter le code existant : si le code faisait vraiment loi, l'action du pirate devait être considérée comme légale. Au vu de cette expérience, le code ne fait donc pas loi sur Ethereum, c'est plutôt la communauté qui fait loi. « Un certain nombre de mineurs ont décidé de revenir au bloc antérieur à la veille de l'attaque. Ils ont fait une croix sur l'immutabilité du code. Ce n'est pas acceptable qu'ils

puissent ainsi réécrire l'histoire, parce qu'ils ont été lésés. C'est étrange, pour ne pas dire dangereux[15] », juge Alain Brégy, d'Aedeus. Si la communauté a décidé de revenir en arrière une fois, pourquoi ne le ferait pas encore, au détriment de ceux dont les transactions seront annulées ? Dans cet épisode, la question de la responsabilité a été esquivée en annulant l'accident. Il semble que personne n'ait été attaqué en justice après cette affaire, sans doute car le pirate, coincé par le fork, n'a pas pu récupérer les fonds. Mais cela ne pourra pas être le cas à chaque fois et des responsables seront désignés par les juges, si les limites des responsabilités de chacun ne sont pas clairement établies au préalable dans ce type d'organisations autonomes décentralisées (DAO). « Ce problème de gouvernance et de personnalité morale opposable n'est pas traité, car l'esprit libertarien y rechigne. Mais on reviendra à des blockchains et des DAO avec des conseils d'administrations et des comités exécutifs[16] », parie Gilles Babinet.

Comment lutter contre la fraude ?

La dernière question juridique qui se pose est celle des contrôles nécessaires pour lutter contre la fraude fiscale, le blanchiment, le financement d'activités illicites et l'achat de biens interdits (drogue, armes, etc.). En l'absence de réglementation précise, les intermédiaires d'achat de cryptomonnaies comme La Maison du Bitcoin ou Paymium s'autorégulent en posant des limites aux volumes d'échange par client et en effectuant des vérifications d'identité. Mais tout le monde ne le fait pas. Certaines très grandes plateformes de change, comme Kraken, n'exigent pas de pièces d'identité en deçà d'un certain montant. « Il y aura forcément des règles plus strictes. La première serait d'obliger les gens qui vendent du Bitcoin à demander une pièce d'identité et à garder trace de chaque transaction », précise Manuel Valente, de La Maison du Bitcoin. Le mouvement général est celui d'un contrôle accru et d'une limitation de l'anonymat des échanges par les gouvernements. Pour lutter contre le blanchiment d'argent et le terrorisme, la Commission européenne a proposé, à l'été 2016, de lister, dans une base de données, les utilisateurs de Bitcoins (sous leur véritable nom et pas sous pseudonyme). Le 10 novembre 2016, un décret gouvernemental français a accru les obligations de vigilance des intermédiaires de paiement en monnaie électronique qui revendent des monnaies (au-dessus de 250 euros stockés ou de 100 euros lors d'une transaction, ils doivent pouvoir identifier leur client). De l'autre côté de l'Atlantique, le fisc américain, l'IRS (Internal Revenue Service), a également resserré l'étau : pour lutter contre l'évasion fiscale, il a déposé, auprès d'un tribunal, une requête pour exiger de Coinbase, l'une des plus grandes plateformes mondiales d'échange de Bitcoins et d'Ethers, les noms de tous ses utilisateurs sur le sol américain, sur les années 2013 à 2015. La plateforme s'y oppose.

Il apparaît nécessaire que l'activité économique en Bitcoins, en Ethers ou en toute autre cryptomonnaie n'échappe pas à la fiscalité, qu'elle soit déclarée et qu'elle puisse être contrôlée. Mais il ne faut pas exagérer l'ampleur du problème. Aux États-Unis par exemple, l'évasion fiscale coûterait au total 458 milliards de dollars par an au gouvernement, selon l'IRS[17]. Or, la capitalisation totale du Bitcoin n'était que de 13,3 milliards de dollars au 14 janvier 2017. Sa responsabilité dans le scandale de

l'évasion fiscale ne peut donc être qu'anecdotique, comparée à celle bien plus grande du système bancaire classique. Quant aux transactions illicites en Bitcoin, elles existent, bien sûr. Mais elles sont moins fréquentes que par le passé, notamment car l'ensemble des transactions d'une adresse publique Bitcoin peut être tracée en un clic : pas très avantageux pour un criminel à la recherche de discrétion. Certaines sociétés se sont même spécialisées dans la surveillance de la blockchain, comme la start-up américaine de cybersécurité Chainalysis, qui traque les fraudeurs pour le compte d'Europol depuis le début de l'année 2016[18]. D'autres cryptomonnaies, plus anonymes encore, ont pris le relais du Bitcoin sur les marchés noirs illégaux, comme Zcash ou Monero, une cyberdevise qui a grimpé en flèche à l'été 2016 et qui occupe depuis le début de 2017 la cinquième place parmi les cryptomonnaies[*1]. « Sur Monero, on ne peut pas tracer les adresses des utilisateurs », souligne Manuel Valente. Idéal pour le blanchiment ou le trafic de drogues.

Réglementer à l'échelle internationale

Les chantiers sont donc nombreux pour les autorités. Devant l'essor de l'activité des blockchains, les pouvoirs publics devront bien s'emparer de ces questions délicates et trouver les règles les mieux adaptées, malgré la difficulté de réglementer des activités naissantes, reposant sur des technologies complexes. Les experts britanniques du Government Office for Science proposent une piste ambitieuse, mais intéressante, à destination des pouvoirs publics : intervenir non pas dans la loi, mais dans le code lui-même. « Le code technique, y compris les logiciels et les protocoles, peut émerger du secteur public. TCP/IP par exemple, ainsi que d'autres protocoles fondamentaux d'Internet, sont issus de projets de recherche financés par des gouvernements et désormais supervisés par l'Internet Society, une ONG internationale […]. Ce n'est pas une solution parfaite, mais cela montre la possibilité d'une implication publique et d'une représentation démocratique dans la production de code – une régulation publique par le code informatique plutôt que par le code juridique[19] », suggère le rapport. Pourquoi ne pas imaginer en effet une régulation coordonnée de quelques blockchains publiques par un ou plusieurs organismes internationaux, comme Internet[*2] ? Cette solution fournirait un début de réponse à la question de la responsabilité, tout en évitant la privatisation du registre.

L'Europe pourrait s'emparer de cette question pour éviter la répétition du scénario d'Internet : « Ce qui fait mal au cœur, c'est que le Web était tout de même une invention européenne [du Britannique Tim Berners-Lee et du Belge Robert Cailliau], qui est passée sous pavillon américain, avec une gouvernance américaine : l'Icann[20] », rappelle Cyril Grunspan, responsable du département d'ingénierie financière à l'Esilv. Cette autorité de régulation, chargée notamment d'attribuer les noms de domaine et les adresses IP des sites Internet, avait été créée par Bill Clinton en 1998 et ne s'est émancipée des États-Unis qu'en septembre 2016. Pas question que la blockchain connaisse le même destin. L'établissement de règles communes, au sein de l'Union européenne, permettrait déjà de donner de la visibilité aux acteurs du secteur et d'éviter une concurrence par le bas entre les pays membres. « Il y a de vrais enjeux de

souveraineté[21] », insiste la députée Laure de La Raudière. « Les pays qui avancent le plus vite prendront les parts de marché au niveau mondial et imposeront leurs règles. Il est temps que l'Europe se réveille. Nous pourrions édicter nous-mêmes des règles, au niveau européen », propose Laure de La Raudière. Les concurrents n'attendent pas. Selon un rapport de l'agence Moody's, « l'autorité de contrôle financier britannique et l'autorité monétaire de Singapour ont chacune annoncé la création de bacs à sable réglementaires [des dispositions allégées temporairement pour permettre la croissance des start-up][22] ».

---

*1. 159 millions de dollars de capitalisation au 14 janvier 2017.

*2. Plusieurs organismes coordonnent le fonctionnement d'Internet et établissent des normes communes : l'Internet Corporation for Assigned Names and Numbers, l'Internet Society, le World Wide Web Consortium…

CHAPITRE 13

Une question de souveraineté pour la France et l'Europe

Une véritable compétition mondiale s'est engagée entre les États-Unis, l'Europe et l'Asie (d'Israël à la Chine), et au sein même de l'Europe, où le Royaume-Uni, l'Estonie, la Suisse, l'Allemagne et la France mènent la danse. Chaque nation redoute de rater le train de cette nouvelle grande révolution technologique. « On ne peut pas reproduire les erreurs du passé et être les colonies des États-Unis en matière d'Internet. On ne peut pas se mettre dans une position protectionniste. Il faut faire gagner la France. Ma conviction, c'est qu'on a tous les talents pour le faire[1] », a lancé Laure de La Raudière, en conclusion des débats au Forum parlementaire de la blockchain. Mais ces talents sont mobiles et il faut leur offrir des conditions adéquates pour que leurs idées se concrétisent. Engagée au niveau mondial, la bataille se joue sur trois terrains complémentaires : la réglementation (nous venons de le voir), mais aussi l'investissement et la recherche. Ces trois facteurs s'imbriquent pour créer un environnement qui attire les projets ou au contraire les fait fuir.

Investissement : l'Europe à la traîne

« Au niveau des investissements, le centre de gravité du secteur se déplace des États-Unis à l'Asie, en sautant l'Europe[2] », a remarqué Philippe Dewost (de la Caisse des dépôts et consignations), lors de la même conférence, avec un peu de dépit : « Pourtant, c'est en Europe qu'on a inventé le *peer-to-peer* et qu'il y a les meilleurs experts en cryptographie. Il faut que l'on arrive à sensibiliser Bruxelles sur la nécessité d'investir sur la blockchain. Il y a une carte à jouer. Les Chinois investissent massivement. Il faudrait mobiliser 500 millions d'euros en Europe en recherche et développement à travers les programmes habituels », suggérait-il à l'assemblée. Lionel Cottu, directeur général d'Elephant Live, qui

prépare l'organisation d'un grand salon professionnel dédié à la blockchain, y voit un enjeu de souveraineté : « Va-t-on enfin rivaliser sur Internet avec les Américains ? Est-on capable d'avoir les Gafa (Google, Apple, Facebook, Amazon) de demain ? Pour cela, il faut des investissements, pas 10 millions d'euros, mais 4 milliards. Aura-t-on l'ambition d'être les numéros 1 mondiaux sur ce sujet[3] ? » s'interroge-t-il. Sur le continent européen, le Royaume-Uni est le pays où il est le plus facile de trouver des fonds pour ce type de projet. « L'écosystème bancaire de Londres est gigantesque, donc ça attire forcément les start-up[4] », témoigne Nicolas Steiner, un investisseur suisse exilé à Londres, membre fondateur du Level39, l'un des plus importants incubateurs de projets financiers en Europe. « Berlin est aussi très dynamique, juge-t-il, mais ce n'est pas un centre financier. » Le Royaume-Uni bénéficie de la présence de la City et d'une politique offensive de son gouvernement, qui veut attirer les projets blockchain sur son territoire. L'ex-ministre des Finances, Georges Osborne, a lancé dès l'été 2014 une étude sur le sujet, visant à positionner Londres comme la capitale mondiale des fintechs. Par comparaison, les nombreuses jeunes pousses françaises peinent à trouver les fonds nécessaires au développement de leurs concepts. « Nous sommes bien équipés en start-up, mais il manque une seule chose : l'argent[5] », déplore Laurent Leloup, fondateur de l'association professionnelle France Blocktech et du site d'information financière Finyear. Au Forum parlementaire de la blockchain, le cofondateur Blockchain France, Antoine Yeretzian, partage ce constat, et avance une explication : « Ceux qui lancent des start-up blockchain en France sont des jeunes développeurs. Aux États-Unis, ce sont plutôt des banquiers, donc ils ont plus de facilités à lever des fonds[6]. » Son intervention s'est terminée sur un vœu sans ambiguïté : « de l'argent pour les start-up ».

Recherche : il est temps d'accélérer

La recherche et l'enseignement constituent le dernier pilier de cette course à l'innovation. « Aux États-Unis, la blockchain a fait l'objet de cours en ligne dès 2013-2014, dont un, excellent, à l'université de Princeton, écrit par Edward Felten, désormais *chief techonology officer* [directeur technique] de la Maison Blanche » relève, admiratif, Cyril Grunspan. La meilleure université d'ingénieurs du monde, le MIT (Massachusetts Institute of Technology), à Boston, a lancé une initiative sur les monnaies numériques, attirant des stars du secteur : « Ils ont embauché le fameux Gavin Andresen, le développeur à la tête de la Fondation Bitcoin, considéré comme l'héritier de Satoshi Nakamoto », salue-t-il. Au Royaume-Uni, un centre de recherche sur les cryptodevises a été ouvert à l'Imperial College de Londres. Dans un rapport publié dès janvier 2016, le gouvernement britannique indique déjà plusieurs objectifs précis à ses chercheurs : « La communauté […] doit s'investir dans la blockchain pour garantir que les registres distribués [synonyme de blockchain] peuvent être étendus à grande échelle, sont sécurisés et fournissent une preuve de véracité de leurs contenus. Ils doivent fournir des opérations de haute performance, à faible délai de latence, appropriés au domaine où la technologie est appliquée. Ils doivent être économes en énergie[7]. » Pendant ce temps, la France prend du retard. « Il n'y a qu'ici qu'on a l'air

de découvrir le sujet. En France, le Bitcoin paraissait trivial, ne méritait pas d'être enseigné. C'est grave pour le monde académique », déplore Cyril Grunspan. Pour compenser ce retard, il a créé, à l'Esilv, une spécialisation fintech et lancé en septembre 2015 le premier cours sur la monnaie numérique cryptomonnaies. Les besoins sont réels. Malgré la qualité reconnue des développeurs français, « les compétences techniques manquent encore[8] », estime Claire Balva, cofondatrice de Blockchain France. « C'est une technologie nouvelle et peu savent coder dessus. » À part Bitcoin, la plupart des blockchains (comme Ethereum) n'ont pas stabilisé leur mode de fonctionnement. « Tous les six mois, des choses changent, il faut se mettre à jour tout le temps, c'est difficile d'être bien formé techniquement », juge-t-elle. Il ne suffit pas de diplômer des spécialistes. L'enjeu est aussi de faire comprendre les opportunités de la blockchain à un public plus large de décideurs d'entreprises, qui doivent assimiler cette innovation pour choisir ou non de s'en saisir. Pour cela, les offres de formation se multiplient. Le premier cours en ligne français sur le sujet a été lancé à la rentrée 2016 par Blockchain France. « L'objectif est de faire comprendre aux managers des moyennes et grandes entreprises ce qu'est cette technologie, d'aborder ses cas d'usage par secteur et de faire réfléchir les participants à des applications chez eux », indique Claire Balva. Finalement, le véritable défi des acteurs de la blockchain est plus grand encore : faire réaliser aux futurs usagers de ces services son formidable potentiel, malgré la complexité apparente de son fonctionnement.

*1. L’ancêtre d’Internet créé en 1969.

*2. « Digital Champion ».

*3. Le protocole qui a permis le passage du réseau Arpanet au réseau Internet, en 1983.

Conclusion

« Il y a l'avenir qui se fait et l'avenir qu'on fait. L'avenir réel se compose des deux[1]. » Cette phrase du philosophe français Alain rappelle que le futur peut être esquissé, mais qu'il n'est pas écrit. L'irruption de la blockchain laisse entrevoir un monde radicalement différent, plus efficace, plus transparent, plus automatisé, où l'individu serait plus libre et mieux considéré comme consommateur, comme travailleur et comme citoyen. Mais l'accomplissement de ces promesses dépend largement de la volonté de chacun de se saisir de cette technologie pour transformer le monde : entrepreneurs et salariés des start-up et des grands groupes, consommateurs, fonctionnaires, hommes politiques, citoyens… Tous ont leur rôle à jouer pour tirer le meilleur de ce nouvel outil technologique.

La blockchain sera-t-elle source de progrès ? Elle peut l'être. Instrument du renforcement du pouvoir de l'individu, elle est un outil de révolte contre les puissances installées : les monopoles, la finance traditionnelle, et même les représentants politiques. Il suffit de s'en saisir pour participer, à son niveau, au basculement des rapports de force aujourd'hui établis. Chacun peut y contribuer. La première étape consiste d'abord à s'intéresser à cette technologie, à en comprendre la logique si nouvelle et déroutante, et à saisir son potentiel. La deuxième est d'expérimenter et de juger, par soi-même, des services déjà existants : par exemple en faisant l'acquisition de quelques centimes de Bitcoins et en achetant quelque chose avec, en enregistrant un document sur un service de notarisation, ou encore en participant à un vote en ligne sur la blockchain. L'ultime étape, pour les plus convaincus, est de créer : identifier ce qui fonctionne mal dans un secteur d'activité que l'on connaît bien, réfléchir à une utilisation de la blockchain qui résolve ce problème et améliore la qualité du service rendu, et tenter de développer une solution viable. Avis aux créateurs de start-up : il est encore temps, le marché n'est pas saturé, beaucoup de bonnes idées restent à trouver !

À ce jour, la blockchain fait l'objet d'un concert de louanges : on aurait tort de s'en priver, rares sont les inventions au potentiel si grand. Mais l'enthousiasme que cette technologie suscite légitimement ne doit pas faire oublier les risques qu'elle présente. Certains s'en inquiètent, comme le théoricien belge du numérique Michel Bauwens, fondateur de la Peer to Peer Foundation, l'une des rares voix dissonantes

sur cette technologie parmi les experts du numérique. « La blockchain participe d'une idéologie qui ne reconnaît pas le collectif, se méfie de la gouvernance démocratique et veut créer des systèmes entièrement tournés vers des individus qui établissent entre eux des contrats automatisés par des algorithmes. Les principes qui sous-tendent le Bitcoin visent à créer un marché universel sans intermédiaire où toute personne est considérée comme un propriétaire souverain[2] », écrivait-il sur son blog. Cette méfiance n'est pas infondée. La blockchain procède en effet d'une vision très particulière de la société, héritée des origines libertariennes du Bitcoin : celle-ci est conçue comme une constellation atomisée de personnes, commerçant entre elles par contrat, au vu de tous, et sans nécessité d'accorder sa confiance à qui que ce soit. Or une société ne peut se réduire à une somme d'individus : elle est elle-même une communauté, qui partage certaines valeurs et certains biens, et est constituée, en son sein, de multiples autres communautés aux frontières mouvantes, qui tissent le lien social nécessaire à la vie en collectivité. En un mot, une société n'est pas un marché. Or, la logique libertarienne, dont est née la blockchain, peut pousser à la considérer comme telle.

Aucune fatalité là-dedans néanmoins : cette technologie n'est pas univoque. Comme Internet avant elle, qui a vu émerger à la fois des services collaboratifs non lucratifs tel Wikipedia et des machines à gagner des milliards comme Facebook, la blockchain donne naissance à des projets aux philosophies très éloignées : il y a un monde entre des PME de paiement installées dans la « cryptovalley » de Zoug, ville la moins imposée de Suisse, dont l'ambition est clairement de gagner vite beaucoup d'argent, et une start-up comme Backfeed, conçue pour promouvoir la coopération des individus, ou encore la fondation Democracy Earth, qui veut réimpliquer les citoyens dans la vie de la cité. N'oublions pas que la blockchain offre aussi de formidables opportunités aux individus pour s'auto-organiser collectivement, sur le terrain, et favoriser le développement d'une économie circulaire (par exemple par la revente d'énergie solaire dans des *smart grids*).

À quoi ressemblera le monde d'après la blockchain ? Impossible de l'affirmer. Mais une chose est sûre : cette technologie est un outil nouveau et puissant, qui permet véritablement d'envisager un renouvellement profond de l'économie, de la société et de la représentation politique. Qui s'en saisira le plus vite et le mieux, pour façonner l'avenir à sa manière ? Peut-être vous.

Notes

Notes de l'introduction « La seconde révolution d'Internet »

1. Propos rapportés par l'ancien directeur marketing et commercial d'Universal, Michel de Souza, le 26 mars 2013.
2. David Lieberman, « CEO Forum : Microsoft's Ballmer Having a Great Time », *USA Today*, 30 avril 2007.
3. Gilles Babinet et Clément Jeanneau, « La Blockchain, une révolution qui va changer le monde », *La Tribune*, 5 février 2016.
4. Floriane Salgues, « Joël de Rosnay : "Nous entrons dans la société de recommandation" », E-marketing.fr, 3 juin 2016.
5. Marc Andreessen, « Why Bitcoin matters », *New York Times*, 21 janvier 2014.
6. Émission *Questions politiques*, France Inter, 2 octobre 2016.
7. Laura Shin, « Bitcoin's Shared Ledger Technology : Money's New Operating System », *Forbes*, 9 septembre 2015.
8. Entretien avec l'auteur, 7 octobre 2016.
9. « Hillary Clinton's Initiative on Technology & Innovation », hillaryclinton.com, 27 juin 2016.
10. Propos recueillis au Forum parlementaire de la blockchain, 4 octobre 2016.
11. Entretien avec l'auteur, 21 juillet 2016.
12. Entretien avec l'auteur, 19 juillet 2016.
13. Entretien avec l'auteur, 26 août 2016.
14. Rapport Capgemini, *Blockchain : A Fundamental Shift for Financial Services Institutions*.

Notes du préambule

1. Satoshi Nakamoto, « Bitcoin P2P e-Cash Paper », satoshi.nakamotoinstitute.org, 1er novembre 2008.
2. www.bitcoin.org/Bitcoin.pdf.
3. Propos recueillis au Forum parlementaire de la blockchain, 4 octobre 2016.

4. Satoshi Nakamoto, « Bitcoin v0.1 released », satoshi.nakamotoinstitute.org, 9 janvier 2009.

5. Satoshi Nakamoto, « Re : Bitcoin v0.1 released », satoshi.nakamotoinstitute.org, 17 janvier 2009.

6. Interview de Milton Friedman par la National Taxpayers Union Fondation, 1999.

7. Satoshi Nakamoto, « Re : Bitcoin P2P e-Cash Paper », satoshi.nakamotoinstitute.org, 7 novembre 2008.

8. Satoshi Nakamoto, « Re : Bitcoin P2P e-Cash Paper », satoshi.nakamotoinstitute.org, 14 novembre 2008.

9. Entretien avec l'auteur, 13 septembre 2016.

10. Robert McMillan, « An Extortionist has been Making Life Hell for Bitcoin's Earlist Adopters », *Wired*, 29 décembre 2014.

11. Andreas Adriano, Hunter Monroe, « The Internet of Trust », *Finance & Development*, IMF, juin 2016.

12. *Ibid*.

13. Nessim Ait-Kacimi, « Bitcoin : de l'ombre à la lumière », *Les Échos*, 1er août 2016.

14. Marc Andreessen, « Why Bitcoin Matters », art. cité.

15. Giulio Prisco, « Financial Blockchain Applications will be Measured in the Trillions, says Blythe Masters at Exponential Finance 2015 », *Bitcoin Magazine*, 4 juin 2015.

16. Entretien avec l'auteur, 20 septembre 2016.

17. « Robust, Cost-Effective Applications Key to Unlocking Blockchain's Potential Credit Benefits », *Moody's Investors Service*, 21 juillet 2016.

Notes du chapitre premier « Qu'est-ce qu'une blockchain ? »

1. Entretien avec l'auteur, 28 juin 2016.

2. Deloitte, EFMA, *Out of the blocks. Blockchain : de la frénésie au prototype* (mai 2016).

3. Pierre Noizat, *Bitcoin, mode d'emploi*, Lulu Entreprises Incorporated, 2015.

Notes du chapitre 2 « Les mécanismes du consensus »

1. Leslie Lamport, Robert Shostak, *The Byzantine Generals Problem*, Marshall Pease, 1982.

2. Sigrid Seibold, George Samman, « Consensus. Immutable Agreement for the Internet of Value », *KPMG*, juin 2016.

3. Propos recueillis au Forum parlementaire de la blockchain, 4 octobre 2016.

4. Entretien avec l'auteur, 21 juillet 2016.

5. Entretien avec l'auteur, 26 juillet 2016.

6. Karl J. O'Dwyer, David Malone, *Etude Bitcoin Mining and its Energy Footprint*, Hamilton Institute and National University of Ireland Maynooth, 26 juin 2014.

7. Satoshi Nakamoto, « Bitcoin : A Peer-to-Peer Electronic Cash System », satoshi.nakamotoinstitute.org, 1er novembre 2008.

8. Pierre Noizat, *Bitcoin, mode d'emploi*, *op. cit.*

9. Sigrid Seibold, George Samman, « Consensus », art. cité.

10. Entretien avec l'auteur, 6 septembre 2016.
11. Pierre Noizat, *Bitcoin, mode d'emploi*, *op. cit.*
12. Nicolas Houy, *It Will Cost You Nothing to "Kill" a Proof-of-Stake Crypto-Currency*, université de Lyon 2, janvier 2014.
13. Entretien avec l'auteur, 27 septembre 2016.
14. Entretien avec l'auteur, 26 juillet 2016.
15. Sigrid Seibold, George Samman, « Consensus », art. cité.

Notes du chapitre 3 « Caractéristiques des blockchains »

1. Cécile Monteil, « La révolution Blockchain : entre fantasme et réalité », *La Tribune*, 8 juillet 2016.
2. Tim Swanson, *Consensus-as-a-Service : A Brief Report on the Emergence of Permissioned, Distributed Systems*, 6 avril 2015.
3. Satoshi Nakamoto, « Bitcoin v0.1 Released », satoshi.nakamotoinstitute.org, 9 janvier 2009.
4. Entretien avec l'auteur, 27 septembre 2016.
5. Vitalik Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform*, décembre 2013.
6. Entretien avec l'auteur, 7 octobre 2016.
7. Entretien avec l'auteur, 18 juillet 2016.
8. Entretien avec l'auteur, 6 septembre 2016.
9. Stéphane Bortzmeyer, « Ethereum. La prochaine étape des systèmes transparents », bortzmeyer.org, 12 septembre 2015.
10. Vitalik Buterin, « Visions, Part 1 : The Value of Blockchain Technology », Blog.ethereum.org, 13 avril 2015.
11. Entretien avec l'auteur, 19 juillet 2016.
12. Deloitte, EFMA, *Out of the Blocks*, *op. cit.*
13. Entretien avec l'auteur, 6 septembre 2016.
14. Richard Brown, « Introducing R3 Corda : a distributed Ledger Designed for Financial Services », Gendal.me, 5 avril 2016.
15. Deloitte, EFMA, *Out of the Blocks*, *op. cit.*
16. Entretien avec l'auteur, 6 septembre 2016.
17. Entretien avec l'auteur, 25 août 2016.
18. Entretien avec l'auteur, 31 août 2016.
19. Entretien avec l'auteur, 22 septembre 2016.

Notes du chapitre 4 « Une révolution financière »

1. Thomas Philippon, *The Future of the Financial Industry*, New York University Stern, 6 novembre 2008.
2. Guillaume Bazot, *La Finance est-elle devenue trop chère ?*, Institut des politiques publiques, juin 2014.
3. Robin Greenwood, David Scharfstein, *The Growth of Modern Finance*, Harvard Business School, juillet 2012.

4. Thomas Philippon, *The Future of the Financial Industry*, *op. cit.*

5. Andreas Adriano, Hunter Monroe, « The Internet of Trust », art. cité.

6. Rapport Capgemini, *Blockchain*, *op. cit.*

7. Santander InnoVentures, « The Fintech 2.0 Paper : Rebooting Financial Services », juin 2015.

8. Capgemini, « Smart Contract in Financial Services, getting from Hype to Reality », 11 octobre 2016.

9. Deloitte, EFMA, *Out of the Blocks*, *op. cit.*

10. Marc Andreessen, « Why Bitcoin Matters », *New York Times*, 21 janvier 2014.

11. Vincent Mignot, « Carte bancaire : le tarif du débit différé de plus en plus avantageux », Cbanque.com, 24 février 2016.

12. Entretien avec l'auteur, 9 septembre 2016.

13. Entretien avec l'auteur, 8 juillet 2016.

14. Anthony Cuthbertson, « Bitcoin now Accepted by 100,000 Merchants Worldwide », *International Business Times*, 4 février 2015.

15. Entretien avec l'auteur, 13 septembre 2016.

16. « ODI & Comic Relief : $1.8bn African Remittance Super Tax », Overseas Development Institute, 22 avril 2014.

17. Entretien avec l'auteur, 26 août 2016.

18. Dilip Ratha, « Trends in Remittances, 2016 : A New Normal of Slow Growth », *World Bank*, 10 juin 2016.

19. Marc Andreessen, « Why Bitcoin Matters », art. cité.

20. Entretien avec l'auteur, 6 octobre 2016.

21. « Massive Drop in Number of Unbanked, says New Report », *World Bank*, 15 avril 2015.

22. Entretien avec l'auteur, 6 octobre 2016.

23. Propos recueillis au Forum parlementaire de la blockchain, le 4 octobre 2016.

24. Entretien avec l'auteur, 28 juin 2016.

25. Entretien avec l'auteur, 22 septembre 2016.

26. Entretien avec l'auteur, 7 septembre 2016.

27. Entretien avec l'auteur, 22 septembre 2016.

28. Entretien avec l'auteur, 6 septembre 2016.

29. Entretien avec l'auteur, 18 juillet 2016.

30. Entretien avec l'auteur, 27 septembre 2016.

31. Entretien avec l'auteur, 8 septembre 2016.

32. « Robust, Cost-Effective… », art. cité.

33. Meghan Elison, « Seven Leading Banks Join Ripple's Global Network », *Ripple*, 22 juin 2016.

34. « Robust, Cost-Effective… », art. cité.

35. « Nasdaq Linq Enables First-Ever Private Securities Issuance Documented with Blockchain Technology », Nasdaq, 30 décembre 2015.

36. « Barclays and Wave Complete World First Blockchain Trade Finance Transaction », Barclays, 7 septembre 2016.

37. « Nasdaq's Blockchain Technology to Transform the Republic of Estonia's e-Residency Shareholder Participation », Nasdaq, 12 février 2016.

38. John Barrdear, Michael Kumhof, « The Macroeconomics of Central Bank Issued Digital Currencies », Bank of England, juillet 2016.

39. data.bitcoinity.org.

40. Wendy Wu, « China's Central Bank Steps up Efforts to Create Digital Currency », *South China Morning Post*, 17 novembre 2016.

41. Chanyaporn Chanjaroen, David Roman, « Singapore to Test Digital Currency in Latest Fintech Initiative », Bloomberg, 16 novembre 2016.

42. Laura Shin, « Canada Has Been Experimenting With A Digital Fiat Currency Called CAD-COIN », *Forbes*, 16 juin 2016.

43. Communiqué Riksbank (Banque centrale de Suède), « Skingsley : Should the Riksbank Issue e-Krona ? », 16 novembre 2016.

44. « Opinion of the European Central Bank, on a Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC », 12 octobre 2016.

45. Yanis Varoufakis, « BITCOIN : A Flawed Currency Blueprint with a Potentially Useful Application for the Eurozone », yanisvaroufakis.eu, 15 février 2014.

46. Oliver Ralph, « Reinsurers Turn to Blockchain Technology », *Financial Times*, 16 mai 2016.

47. Entretien avec l'auteur, 8 septembre 2016.

48. Entretien avec l'auteur, 9 juillet 2016.

49. Entretien avec l'auteur, 7 septembre 2016.

50. Entretien avec l'auteur, 6 septembre 2016.

51. Capgemini, « Smart Contract in Financial Services… », art. cit.

52. Entretien avec l'auteur, 15 septembre 2016.

53. Entretien avec l'auteur, 22 septembre 2016.

Notes du chapitre 5 « Une vraie économie du partage »

1. Propos rapportés par Quentin Hardy, « The Web's Creator Looks to Reinvent It », *New York Times*, 7 juin 2016.

2. Entretien avec l'auteur, 22 juillet 2016.

3. Vitalik Buterin, « Bootstrapping a Decentralized Autonomous Corporation, Part 3 : Identity Corp », blog.ethereum.org, 31 décembre 2013.

4. Entretien avec l'auteur, 26 septembre 2016.

5. https://the-federation.info/

6. Will Oremus, « The Search for the Anti-Facebook », *Slate*, 28 octobre 2014.

7. Neil Strauss, « Can this Social Media Site Make you Rich ? », *Rolling Stone*, 11 novembre 2016.

8. « cyber.Fund to launch the first Russian-language social network based on blockchain », Bitcoinconf.moscow.

9. andrew0, « Steemit Posts on the Blockchain : How to Delete Them ? », steemit.com.

10. Philippe Mabille, « Pour le fondateur de Airbnb, la *share economy* a un avenir brillant », *La Tribune*, 23 janvier 2014.

11. Giana M. Eckhardt, Fleura Bardhi, « The Sharing Economy Isn't About Sharing at All », *Harvard Business Review*, 28 janvier 2015.

12. Arcade City, « Ridesharing Startup Arcade City Launches in 27 States », 14 mars 2016.

13. Ivan Chen-O'Neill, « An American Fraudster : The Dirge of Christopher David, CEO of Arcade City », Medium, 2 avril 2016.

14. Arcade City, @Arcadecityhall, Facebook, 2 avril 2016.

15. Entretien avec l'auteur, 22 septembre 2016.

16. Simon Polrot, « Slock.it : la promesse des objets connectés sur la blockchain », Ethereum France, 4 avril 2016.

17. Forrester Research, « The Public Cloud Services Market Will Grow Rapidly To $236 Billion In 2020 », 1er septembre 2016.

18. Mary-Ann Russon, « ZeroNet : A Revolutionary New Decentralised p2p Internet for a Post-Edward Snowden World », *International Business Times UK*, 12 septembre 2016.

19. Pierre Breteau, « “Streaming” musical : combien touchent les artistes ? », *Le Monde*, 25 juin 2015.

20. « Midem/Adami : pour un meilleur partage de la valeur pour la musique en ligne », Irma.asso.fr, 1er février 2013.

21. D. A. Wallach, « Bitcoin for Rockstars. How Cryptocurrency Can Revolutionize The Music Industry », *Backchannel*, 10 décembre 2014.

22. Entretien avec l’auteur, 29 juillet 2016.

23. Jeremy Gordon, « Thom Yorke Releases New Album Tomorrow’s Modern Boxes Via BitTorrent », Pitchfork, 26 septembre 2014.

24. Lily Kuo, « Imogen Heap Wants to Use Blockchain Technology to Revolutionize the Music Industry », *Quartz*, 19 février 2016.

25. Yessi Bello Perez, « Imogen Heap : Decentralising the Music Industry with Blockchain », *Tech City News*, 14 mai 2016.

26. Entretien avec l’auteur, 18 juillet 2016.

27. Entretien avec l’auteur, 21 juillet 2016.

28. Pierre-François Racine, Conseil supérieur de la propriété littéraire et artistique, Lettre de mission du 8 juillet 2016.

29. Marc Andreessen, « Why Bitcoin Matters », art. cité.

30. « Robust, Cost-Effective… », art. cité.

31. Source ACPM, octobre 2016.

32. Entretien avec l’auteur, 28 août 2016.

33. A. C. Eveillé, « Guillaume lance Bitcoin Bandit, un jeu sur application mobile », *La Dépêche*, 25 août 2016.

34. Entretien avec l’auteur, 18 juillet 2016.

35. Entretien avec l’auteur par mail, 28 septembre 2016.

36. Entretien avec l’auteur, 6 septembre 2016.

Notes du chapitre 6 « Un tremplin vers un monde automatisé »

1. Gartner, « Gartner Says 6.4 Billion Connected “Things” Will Be in Use in 2016, Up 30 Percent From 2015 », 10 novembre 2015.

2. Idate, « Internet of Things », 31 octobre 2015.

3. Entretien avec l’auteur, 9 juillet 2016.

4. Entretien avec l’auteur, 26 juillet 2016.

5. Entretien avec l’auteur, 6 septembre 2016.

6. Entretien avec l’auteur, 26 juillet 2016.

7. Entretien avec l’auteur, 26 août 2016.

8. Entretien avec l’auteur, 25 juillet 2016.

9. Florian Debes, « Les blockchains “dans la vraie vie” des entreprises », *Les Échos*, 15 juin 2016.

10. Stan Higgins, « How Bitcoin Brought Electricity to a South African School », CoinDesk, 9 mars 2016.

11. Coinmarketcap, 25 novembre 2016.

12. Thomas Blosseville, « Énergie solaire : les premiers SolarCoins distribués en France », environnement-magazine.fr, 24 octobre 2016.

13. « Bouygues Immobilier s’associe à Stratumn pour déployer une blockchain pour *smart grid* », communiqué de presse, 4 octobre 2016.

14. Ridha Loukil, « Bouygues Immobilier mise sur la Blockchain pour tracer les échanges d'énergie solaire », L'Usine digitale, 10 octobre 2016.

15. Entretien avec l'auteur, 22 septembre 2016.

16. Paul Benkimoun, « Essai clinique mortel de Rennes : un rapport pointe le manque d'information des volontaires », *Le Monde*, 22 mai 2016.

17. Yves Eudes, « La blockchain sort de la sphère financière pour entrer dans l'industrie », *Le Monde*, 11 juillet 2016.

18. John Holden, Greg Irving, « How Blockchain-Timestamped Protocols Could Improve the Trustworthiness of Medical Science », F1000 Research, 2016.

19. « Return of the Blood Diamond », Global Witness, 14 avril 2010.

20. Leanne Kemp (UK Government Office for Science), « Distributed Ledger Technology : Beyond Block Chain », janvier 2016.

21. Entretien avec l'auteur, 23 août 2016.

Notes du chapitre 7 « Un pilier pour la démocratie et l'administration de demain »

1. Al Gore, *Inauguration of the First World Telecommunication Development Conference*, 21 mars 1994.

2. Pia Mancini, « Comment mettre à jour la démocratie à l'ère d'Internet ? », Ted Talks, octobre 2014.

3. Jean-Baptiste de Montvalon, « Pour une majorité de Français, la démocratie fonctionne de moins en moins bien », *Le Monde*, 7 novembre 2016.

4. Yascha Mounk, Roberto Stefan Foa, « The Signs of Democratic Deconsolidation », *Journal of Democracy*, rapporté dans Gwynn Guilford, « Harvard Research Suggests that an Entire Global Generation Has Lost Faith in Democracy », *Quartz*, 30 novembre 2016.

5. Willem-Jan Hengeveld, « Nedap/Groenendaal ES3B Voting Computer, a Security Analysis », Rop Gonggrijp, 6 octobre 2006.

6. Lawrence Norden, Christopher Famighetti, « America's Voting Machines at Risk », Brennan Center for Justice, 15 septembre 2015.

7. Alain Anziani, Antoine Lefèvre, *Rapport d'information*, 9 avril 2014.

8. Homeland Security, « Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security », 7 octobre 2016.

9. Romain Rouphael, « Voter *via* la blockchain : expérimentations et retours d'expérience », LinkedIn, 2 mai 2016.

10. Entretien avec l'auteur, 27 septembre 2016.

11. Propos recueillis au Forum parlementaire de la blockchain, 4 octobre 2016.

12. Entretien avec l'auteur, 14 décembre 2016.

13. Chris Duckett, « Australia Post Details Plan to use Blockchain for Voting », ZDNet, 22 août 2016.

14. Vabariigi Valimiskomisjon, « Statistics about Internet voting in Estonia », http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics (consulté le 29 janvier 2017).

15. Leanne Kemp (UK Government Office for Science), « Distributed Ledger Technology », art. cité.

16. Entretien avec l'auteur, 27 septembre 2016.

17. Entretien avec l'auteur, 26 août 2016.

18. e-Estonia.com, Facts.

19. Propos recueillis au Forum parlementaire de la blockchain, le 4 octobre 2016.

20. Baromètre Digital Gouv 2016, Ipsos pour Sopra Steria, 15 novembre 2016.

21. Entretien avec l'auteur, le 6 octobre 2016.

22. Leanne Kemp (UK Government Office for Science), « Distributed Ledger Technology », art. cité.

23. « Robust, Cost-Effective… », art. cité.

24. « Deep Shift. Technological tipping points and societal impacts », The World Economic Forum, septembre 2015.

25. Honoré de Balzac, *Le Notaire*, 1840.

26. Ordonnance n° 45-2590 du 2 novembre 1945 relative au statut du notariat.

27. Entretien avec l'auteur, 24 juillet 2016.

28. Laura Shin, « Republic Of Georgia To Pilot Land Titling On Blockchain with Economist Hernando De Soto », BitFury, 21 avril 2016.

29. « The BitFury Group Announces Launch of Breakthrough Blockchain Land Titling Project in the Republic of Georgia », Medium, 22 avril 2016.

30. Entretien avec l'auteur, 24 août 2016.

31. *Honduras to build land title registry using Bitcoin technology*, Gertrude Chavez-Dreyfuss, 15 mai 2015

32. Entretien par mail avec l'auteur, 15 septembre 2016.

33. Florian Mantione Institut, « Septième étude sur les CV trompeurs », février 2013.

34. Entretien par mail avec l'auteur, 18 juillet 2016.

35. Entretien avec l'auteur, 5 septembre 2016.

36. Entretien avec l'auteur, 7 septembre 2016.

37. Entretien avec l'auteur, 24 juillet 2016.

Notes de la troisième partie « LES DÉFIS DE LA BLOCKCHAIN »

1. Entretien avec l'auteur, 31 août 2016.

2. Entretien avec l'auteur, 7 octobre 2016.

Notes du chapitre 8 « Développer des systèmes moins énergivores »

1. Sebastiaan Deetman, « Bitcoin Could Consume as Much Electricity as Denmark by 2020 », Motherboard, 29 mars 2016.

2. « Promesses et limites de la technologie "blockchain", nouvel Eldorado de la finance », AFP, 9 août 2016.

3. Rob Price, « Look Inside the Surreal World of an Icelandic Bitcoin Mine, where they Literally Make Digital Money », Business Insider, 20 août 2015.

4. Données du *New York Times*, du 24 mai au 26 juin 2016 ; Nathaniel Popper, « How China Took Center Stage in Bitcoin's Civil War », *New York Times*, 29 juin 2016.

5. SolarCoin, « SolarCoin modifie son Blockchain et passe en mode POST (Proof of Stake Time) », 24 juillet 2015.

6. Propos recueillis au Forum parlementaire de la blockchain, 4 octobre 2016.

Notes du chapitre 9 « Rapidité, confidentialité, sécurité : trois défis techniques »

1. Estimation sur la base des résultats de Paypal au troisième trimestre 2016, Paypal, *PayPal Reports Strong Third Quarter Results*, 20 octobre 2016.
2. Entretien avec l'auteur, 28 août 2016.
3. Gertrude Chavez-Dreyfuss, « Cyber Threat Grows for Bitcoin Exchanges », Reuters, 29 août 2016.
4. Entretien avec l'auteur, 21 juillet 2016.
5. Propos recueillis au Forum parlementaire de la blockchain, 4 octobre 2016.
6. Entretien avec l'auteur, 27 septembre 2016.

Note du chapitre 10 « Marketing : trouver des modèles économiques viables sans se renier »

1. Entretien avec l'auteur, 13 septembre 2016.

Notes du chapitre 11 « Transformer l'emploi sans le détruire »

1. Entretien avec l'auteur, 6 septembre 2016.
2. Michael Chui, James Manyika, Mehdi Miremadi, *Four Fundamentals of Workplace Automation*, McKinsey Quarterly, novembre 2015.
3. Entretien avec l'auteur, 24 juillet 2016.
4. John Maynard Keynes, *Lettre à mes petits-enfants*, 1931.
5. Entretien avec l'auteur, 25 juillet 2016.
6. *Bootstrapping A Decentralized Autonomous Corporation : Part I*, Vitalik Buterin, blog.ethereum.org, 31 décembre 2013.

Notes du chapitre 12 « Réglementer sans freiner l'innovation »

1. Propos recueillis au Forum parlementaire de la blockchain, le 4 octobre 2016.
2. *Ibid*.
3. Entretien avec l'auteur, 21 juillet 2016.
4. Propos recueillis au Forum parlementaire de la blockchain, le 4 octobre 2016.

5. *Ibid.*
6. *Ibid.*
7. Deloitte, EFMA, *Out of the Blocks*, *op. cit.*
8. « Quelle est la nature juridique de Bitcoin ? », Bitcoin.fr, 30 octobre 2015.
9. Propos recueillis au Forum parlementaire de la blockchain, le 4 octobre 2016.
10. *Ibid.*
11. Entretien avec l'auteur, 24 juillet 2016.
12. Entretien avec l'auteur, 25 août 2016.
13. Entretien avec l'auteur, 20 septembre 2016.
14. Entretien avec l'auteur, 19 juillet 2016.
15. Entretien avec l'auteur, 26 juillet 2016.
16. Entretien avec l'auteur, 31 août 2016.
17. Chris Matthews, « Here's How Much Tax Cheats Cost the U.S. Government a Year », *Fortune*, 29 avril 2016.
18. « Blockchain Cybersecurity Startup Chainalysis inks MoU with Europol », Finextra.com, 19 février 2016.
19. Leanne Kemp (UK Government Office for Science), « Distributed Ledger Technology », art. cité.
20. Entretien avec l'auteur, 21 juillet 2016.
21. Entretien avec l'auteur, 19 juillet 2016.
22. « Robust, Cost-Effective… », art. cité.

Notes du chapitre 13 « Une question de souveraineté pour la France et l'Europe »

1. Propos recueillis au Forum parlementaire de la blockchain, 4 octobre 2016.
2. *Ibid.*
3. Entretien avec l'auteur, 23 juillet 2016.
4. Entretien avec l'auteur, 8 septembre 2016.
5. Entretien avec l'auteur, 20 juillet 2016.
6. Propos recueillis au Forum parlementaire de la blockchain, 4 octobre 2016.
7. Leanne Kemp (UK Government Office for Science), « Distributed Ledger Technology », art. cité.
8. Entretien avec l'auteur, 25 août 2016.

Notes de la conclusion

1. Alain, *Propos sur le bonheur*, 1923.

2. Michel Bauwens, *Blockchain. Du rêve technocratique à l'outil émancipateur ?*, blogfr.p2pfoundation.net, 2 mai 2016.

Remerciements

Merci à Madame Axelle Lemaire, l'ancienne secrétaire d'État chargée du numérique et de l'innovation, d'avoir accepté de partager son expertise et sa vision de la blockchain dans la préface.

Merci infiniment à chacun des 48 experts qui ont eu la gentillesse et la patience de m'expliquer leurs projets et leurs visions de cette passionnante technologie.

Stephan Tual, cofondateur de Slock.it,

Anna Piperal, directrice du *showroom* e-Estonia,

Martin Ruubel, responsable des activités de « gouvernement numérique » chez Guardtime,

Peronet Despeignes, responsable des opérations spéciales chez Augur,

Nicolas Houy, économiste au CNRS,

Louis Margot-Duclot, fondateur de OpenOrg.co, porte-parole en France de Democracy Earth,

Brian Hoffman, fondateur d'OpenBazaar,

Nadia Filali, responsable des activités Blockchain au sein de la Caisse des dépôts et consignations et copilote de l'initiative Labchain,

François Dorléans, directeur des opérations et cofondateur de Stratumn,

Abhi Dobhal, vice-président en charge du Business Development chez Factom,

Adrian Sauzade, cocréateur de Wekeep.io et fondateur de Czam,

Nicolas Steiner, investisseur spécialiste des fintechs et cofondateur de l'accélérateur de start-up financières Level39,

Laurent Benichou, directeur de l'innovation et de la prospective chez Axa,

Simon Polrot, fondateur du site Ethereum France et avocat au cabinet Fieldfisher,

Joan Noguera, représentant en France de BTC facil,

Luca Comparini, responsable blockchain d'IBM France,

Quentin de Beauchesne, fondateur de Ledgys,

Gilles Babinet, représentant du numérique pour la France auprès de la Commission européenne,

Chris Bates, *chief security officer* de Bitland,

Matan Field, cofondateur de Backfeed,

Guy Zyskind, cofondateur d'Enigma,

Bill Barhydt, PDG d'Abra,

Michel Bauwens, fondateur de la Peer to Peer Foundation,

Claire Balva, cofondatrice de Blockchain France,

Leanne Kemp, fondatrice d'Everledger,

Phil Barry, coondateur d'Ujo et fondateur de Blokur,

Bruno Guez, fondateur de Revelator,

Alain Brégy, cofondateur d'Aedeus,

Primavera De Filippi, chargée de recherche au CNRS et au Berkman Center for Internet and Society, de l'université d'Harvard,

John Lilic, conférencier et expert de l'utilisation de la blockchain dans le secteur de l'énergie chez Consensys,

Louison Dumont, fondateur de Bitproof,

Cyril Grunspan, responsable du département d'ingénierie financière de l'Esilv,

Pierre Noizat, fondateur de Paymium,

Lionel Cottu, directeur général d'Elephant Live,

Laurent Leloup, fondateur du site Finyear,

Corinne Erhel, députée PS des Côtes-d'Armor,

Laure de La Raudière, députée LR d'Eure-et-Loir,

Joseph Lubin, fondateur de Consensys,

Julien Barbier, cofondateur de la Holberton School of Software Engineering,

Éric Lévy-Bencheton, expert blockchain au cabinet de conseil Keyrus,

Emmanuel Méthivier, président du CA Store (Crédit agricole),

Manuel Valente, directeur de la Maison du Bitcoin,

Ming Chan, directrice de la fondation Ethereum,

Niklas Nikolajsen, fondateur de Bitcoin Suisse,

Martin Würmli, directeur des services municipaux de la ville de Zoug (Suisse),

David Guez, fondateur de LaPrimaire.org,

Vitus Amman, directeur Marketing de Monetas,

l'équipe anonyme de BitBet.

DU MÊME AUTEUR

Lady Gaga, 10/18, coll. « Le monde expliqué aux vieux », 2013.

Retrouvez tous nos ouvrages
sur www.tallandier.com